UNIVERSITÀ DI PISA

Dipartimento di Matematica

Corso di Laurea Triennale in Matematica

Il problema inverso di Galois

Un approccio geometrico al problema

Relatore:

Davide Lombardo

Candidato:

Matteo Poletto

ANNO ACCADEMICO 2023/2024

Indice

SEC. 1 — INTRODUZIONE

Il problema inverso di Galois consiste nel trovare, dato un gruppo finito G, un'estensione di Galois di $\mathbb{Q}$ che abbia G come gruppo di Galois. Il problema è tutt'ora un problema aperto, ma è stato risolto per alcune famiglie di gruppi. Uno degli obiettivi di questa tesi è presentare un approccio, sviluppato principalmente da Emmy Noether, David Hilbert, e portato avanti in seguito da Jean-Pierre Serre, che permette di risolvere il problema inverso di Galois nei casi in cui G appartenga ad alcune famiglie di gruppi. Fra queste, ad esempio, ci sono i gruppi abeliani e i gruppi della forma S_n e A_n. La referenza principale per l'approccio che ora esponiamo è [1].

L'approccio in questione si compone di due parti, una di natura più geometrica e una di natura più algebrica. La prima parte consiste nel trovare un'estensione di Galois F di un campo della forma $\mathbb{Q}(T_1, T_2, ..., T_n)$ con gruppo G. Il metodo più utilizzato per trovare queste estensioni è quello di cercare rivestimenti (possibilmente ramificati) tra varietà algebriche che inducano l'inclusione di campi sopra descritta, ovvero mappe $X \to Y$ con X, Y varietà algebriche e Y tale che $\mathbb{Q}(Y) = \mathbb{Q}(T_1, T_2, ..., T_n)$. Questa costruzione fornisce un'inclusione di campi $\mathbb{Q}(Y) \hookrightarrow \mathbb{Q}(X)$ che è un'estensione di Galois.

La seconda parte, invece, consiste nel trovare un'estensione di Galois di $\mathbb{Q}$ con gruppo G, data un'estensione di Galois $F : \mathbb{Q}(T_1, T_2, ..., T_n)$ con gruppo G. Questo è possibile grazie al teorema di irriducibilità di Hilbert. In realtà il teorema di irriducibilità di Hilbert, sotto alcune ipotesi sul campo F, ci permette di trovare infinite estensioni di Galois di $\mathbb{Q}$, data una sola estensione di $\mathbb{Q}(T_1, T_2, ..., T_n)$, il che rende questo approccio particolarmente interessante, in quanto permette di trovare intere famiglie di polinomi che diano un certo gruppo di Galois.
Da notare che la seconda parte dell'approccio è indipendente dal gruppo G che stiamo considerando, la differenza tra i vari gruppi sta nella prima parte, in cui per ogni gruppo bisogna trovare uno specifico rivestimento di varietà che lo realizzi.

L'obiettivo di questa tesi è presentare l'approccio sopra menzionato e mostrare come costruire dei rivestimenti di varietà algebriche che risolvano il problema per tutti i gruppi abeliani. Infine, mostreremo più esplicitamente come realizzare un rivestimento che dia vita ad un'estensione con gruppo di Galois $\mathbb{Z}/5\mathbb{Z}$.

sec. 2 — L'approccio generale

2.1. Il teorema di irriducibilità di Hilbert

L'approccio al problema inverso di Galois che vedremo è stato portato avanti in larga parte anche da David Hilbert, al quale si deve il teorema grazie a cui ci è possibile trovare un'estensione di Galois di $\mathbb{Q}$ data un'estensione di Galois di $\mathbb{Q}(T_1, T_2, ..., T_m)$ (in realtà vedremo più avanti che saremo in grado di ottenere infinite estensioni di $\mathbb{Q}$, data un'estensione di $\mathbb{Q}(T_1, ..., T_m)$).

Il teorema, nella versione che utilizzeremo noi, è il seguente

Teorema 2.1 (Hilbert): Dato un polinomio irriducibile in $m+1$ variabili $f(x, T_1, T_2, ..., T_m) \in \mathbb{Z}[x, T_1, T_2, ..., T_m] \setminus \mathbb{Z}[T_1, T_2, ..., T_m]$, è sempre possibile sostituire alle variabili $T_1, T_2, ..., T_m$ una m-upla di numeri interi $(t_1, ..., t_m) \in \mathbb{Z}^m$ in modo tale che il polinomio $f(x, t_1, ..., t_m) \in \mathbb{Z}[x]$ non sia scomponibile come prodotto di fattori di grado positivo in $\mathbb{Z}[x]$.
Inoltre esistono infinite m-uple $(t_1, ..., t_m) \in \mathbb{Z}^m$ tali che il polinomio $f(x, t_1, ..., t_m) \in \mathbb{Z}[x]$ non sia scomponibile come prodotto di fattori di grado positivo in $\mathbb{Z}[x]$.

Corollario 2.1.1: Dato un polinomio irriducibile in $m+1$ variabili $f(x, T_1, T_2, ..., T_m) \in \mathbb{Z}[x, T_1, T_2, ..., T_m] \setminus \mathbb{Z}[T_1, T_2, ..., T_m]$ e dato un polinomio $a(T_1, ..., T_m) \in \mathbb{Q}[T_1, ..., T_m]$, esistono infinite m-uple $(t_1, ..., t_m) \in \mathbb{Z}^m$ tali che il polinomio $f(x, t_1, ..., t_m) \in \mathbb{Z}[x]$ non sia scomponibile come prodotto di fattori di grado positivo in $\mathbb{Z}[x]$ e tali che $a(t_1, ..., t_m) \neq 0$.

Per chiarezza, quando utilizzeremo il termine "specializzare" una variabile ad un valore intenderemo sostituire quel dato numero al posto della variabile in questione. Nell'enunciato di questo teorema potremmo dire che "è possibile specializzare le variabili $T_1, ..., T_m$ a infinite m-uple di interi, in modo tale che il polinomio resti irriducibile (come prodotto di fatotri di grado positivo)".

§ 2.1.i. Il caso con due variabili —

Vediamone una dimostrazione, prima nel caso in cui $m = 1$, e poi nel caso generale. Ci concentreremo prima sulla seguente versione del teorema:

Teorema 2.2: Dato un polinomio irriducibile in 2 variabili $f(x, T) \in \mathbb{Z}[x, T] \setminus \mathbb{Z}[T]$, è possibile sostituire alla variabile T infiniti numeri interi t in modo tale che il polinomio $f(x, t) \in \mathbb{Z}[x]$ non sia scomponibile come prodotto di fattori di grado positivo in $\mathbb{Z}[x]$.

In realtà dimostreremo la contronominale, ovvero

Teorema 2.3: Dato un polinomio in 2 variabili $f(x, T) \in \mathbb{Z}[x, T] \setminus \mathbb{Z}[T]$, se esiste t_0 tale che $\forall t_1 \geq t_0$ il polinomio $f(x, t_1)$ è scomponibile come prodotto di fattori di grado positivo in $\mathbb{Z}[x]$, allora $f(x, T)$ è riducibile in $\mathbb{Z}[x, T]$.

Spezziamo la dimostrazione in diversi passaggi, il primo dei quali sarà formulare un enunciato leggermente più debole che dimostreremo essere equivalente a quello appena dato.

§ 2.1.i.i. Enunciato equivalente —

Teorema 2.4: Dato un polinomio in 2 variabili $f(x,T) \in \mathbb{Z}[x,T] \setminus \mathbb{Z}[T]$, se esiste t_0 tale che $\forall t_1 \geq t_0$ il polinomio $f(x,t_1)$ è monico e scomponibile come prodotto di fattori di grado positivo in $\mathbb{Z}[x]$, allora $f(x,T)$ è riducibile in $\mathbb{Q}[x,T]$.

Proposizione 2.1.1: Il Teorema 2.4 è equivalente al Teorema 2.3.

Sia $f(x,T)$ un polinomio in $\mathbb{Z}[x,T] \setminus \mathbb{Z}[T]$, per cui esiste t_0 tale che $\forall t_1 \geq t_0$ il polinomio $f(x,t_1)$ è scomponibile come prodotto di fattori di grado positivo in $\mathbb{Z}[x]$. Assumiamo che valga il Teorema 2.4 e dimostriamo che allora $f(x,T)$ è riducibile in $\mathbb{Z}[x,T]$.

Poiché $f(x,T) \in \mathbb{Z}[x,T] \setminus \mathbb{Z}[T]$, possiamo scriverlo nella forma

$$f(x,T) = R(T)x^n + R_1(T)x^{n-1} + ... + R_{n-1}(T)x + R_n(T) \tag{1}$$

con $n \geq 1$ e in cui R, R_j sono polinomi in $\mathbb{Z}[T]$.
Definiamo il seguente polinomio

$$g(x,T) = R(T)^{n-1} f\left(\frac{x}{R(T)}, T\right) = x^n + S_1(T)x^{n-1} + ... + S_{n-1}(T)x + S_n(T) \tag{2}$$

in cui $S_j(T) = R_j(T)R(T)^{j-1}$.
Notiamo in particolare che $g(x,T)$ è un polinomio monico ed è a sua volta in $\mathbb{Z}[x,T] \setminus \mathbb{Z}[T]$.

Prima di procedere con la dimostrazione della Proposizione 2.1.1 dimostriamo il seguente lemma

Lemma 2.1.2:

a) (Gauss) Un polinomio in $\mathbb{Z}[x]$ è irriducibile in $\mathbb{Z}[x]$ se e solo se è irriducibile in $\mathbb{Q}[x]$ e il massimo comune divisore dei suoi coefficienti è 1. (In particolare un polinomio in $\mathbb{Z}[x]$ è scomponibile come prodotto di fattori di grado positivo in $\mathbb{Z}[x]$ se e solo se è riducibile in $\mathbb{Q}[x]$)

b) Un polinomio $\psi(T)$ divide un polinomio $f \in \mathbb{Z}[x,T]$ se e solo se, scrivendo

$$f(x,T) = a_0(T)x^n + a_1(T)x^{n-1} + ... + a_{n-1}(T)x + a_n(T) \tag{3}$$

il polinomio $\psi(T)$ divide ciascun coefficiente $a_j(T)$.

c) Se $f(x,T) \in \mathbb{Z}[x,T]$ può essere scomposto nel prodotto di due polinomi in $\mathbb{Q}(T)[x]$, allora può essere scomposto anche nel prodotto di due polinomi di grado positivo in $\mathbb{Z}[x,T]$.

Dimostrazione:

a) E' un famoso risultato dovuto a Gauss.

b) Notiamo che se un polinomio $\psi(T)$ divide $f(x,T)$, allora possiamo scrivere

$$\begin{gathered} f(x,T) = \psi(T)\ (h(T)x^n + ... + h_{n-1}(T)x + h_n(T)) = \\ \psi(T)h(T)x^n + ... + \psi(T)h_{n-1}(T)x + \psi(T)h_n(T) \end{gathered} \tag{4}$$

Questo implica che $\psi(T)$ divide ogni coefficiente $a_j(T)$ di $f(x,T)$.

c) Data una scomposizione di $f(x,T)$ in $\mathbb{Q}(T)[x]$, per ognuno dei due fattori, raccogliamo il denominatore comune dei coefficienti in $\mathbb{Q}(T)$ e riscriviamo i due polinomi come rapporto tra un polinomio in $\mathbb{Z}[x,T]$ e un polinomio in $\mathbb{Z}[T]$. Dunque otteniamo una scomposizione della forma

$$f(x,T) = \frac{f_1(x,T)}{\varphi_1(T)} * \frac{f_2(x,T)}{\varphi_2(T)} \tag{5}$$

dove $f_1, f_2 \in \mathbb{Z}[x,T]$ e $\varphi_1, \varphi_2 \in \mathbb{Z}[T]$ tali che f_1 non sia divisibile per nessun fattore di φ_1 e analogamente per f_2 con φ_2. Ne segue che tutti i fattori di φ_2 dovranno dividere f_1 e tutti i fattori di φ_1 dovranno dividere f_2.
Ma per il punto b), questo implica che φ_2 divide ogni coefficiente di f_1, visto come polinomio in $\mathbb{Z}[T][x]$, da cui

$$\frac{f_1(x,T)}{\varphi_2(T)} \in \mathbb{Z}[x,T] \tag{6}$$

da cui la tesi.

□

Siamo finalmente pronti a dimostrare la Proposizione 2.1.1

Dimostrazione: (Proposizione 2.1.1)

Sia $f(x,T) \in \mathbb{Z}[x,T] \setminus \mathbb{Z}[T]$ un polinomio tale che esista t_0 per cui $\forall t_1 \geq t_0$ il polinomio $f(x,t_1)$ è riducibile in $\mathbb{Z}[x]$.
Sia $g(x,T)$ definito nell' Equazione (2) . Abbiamo visto che $g(x,T)$ è monico e a coefficienti interi. Dalla definizione di $g(x,T)$, è facile notare che se $f(x,t_1)$ e fattorizzabile in $\mathbb{Z}[x]$, allora $g(x,t_1)$ è fattorizzabile in $\mathbb{Q}[x]$. Ma essendo $g(x,t_1)$ monico e a coefficienti interi, il punto a) del Lemma 2.1.2 ci dice che $g(x,t_1)$ è fattorizzabile in $\mathbb{Z}[x]$ come prodotto di fattori di grado positivo.
Dunque $g(x,T)$ rispetta tutte le ipotesi del Teorema 2.4, da cui deduciamo che

$$g(x,T) = \psi(x,T) * \psi'(x,T) \tag{7}$$

con $\psi, \psi' \in \mathbb{Q}[x,T]$. Da questa relazione otteniamo

$$R(T)^{n-1} f(x,T) = g(xR(T),T) = \psi(xR(T),T) * \psi'(xR(T),T) = \frac{\varphi(x,T) * \varphi'(x,T)}{A} \tag{8}$$

in cui abbiamo raccolto il denominatore comune ai coefficienti di ψ e ψ', in modo da ottenere $\varphi, \varphi' \in \mathbb{Z}[x,T]$ e $A \in \mathbb{Z}$. Dunque abbiamo

$$f(x,T) = \frac{\varphi(x,T) * \varphi'(x,T)}{AR(T)^{n-1}} \tag{9}$$

e concludiamo per il punto c) del Lemma 2.1.2. □

§ 2.1.i.ii. Il teorema di Puiseux —

Per proseguire abbiamo bisogno di un risultato che ci permetta, dato il polinomio $f(x,T)$, di scriverci le radici di f, visto come polinomio in x a coefficienti in $\mathbb{Z}[T]$, in funzione di T.
Introduciamo la seguente definizione:

Definizione 2.1.3: Una serie di Puiseux a infinito è una serie formale

$$u(x) = \sum_{i=-h}^{\infty} \frac{B_i}{x^{\frac{i}{k}}} \tag{10}$$

in cui $h \in \mathbb{Z}, k \in \mathbb{Z}_{>0}$ e $B_i \in \mathbb{C}$. Una tale serie si dice convergente se esiste c tale che $\forall x, |x| \geq c$ la serie converge.

Osservazione 2.1.4: Da notare che ogni numero complesso x ha k diverse radici k-esime, per cui quando diciamo che una serie u converge in x intendiamo che per ogni scelta di una radice k-esima λ di x, la serie $u(x)$ calcolata sostituendo $x^{\frac{i}{k}}$ con λ^i converge.

Osservazione 2.1.5: Le serie di Puiseux formano un campo.

Osservazione 2.1.6: Le serie di Puiseux convergenti formano a loro volta un campo.

Dimostrazione: Se due serie $a(x)$ converge per $|x| \geq c$ e $b(x)$ converge per $|x| \geq c'$, allora la somma, la differenza e il prodotto convergono per $|x| \geq \max(c, c')$. Per quanto riguarda il rapporto ci interessa che $b(x) \neq 0$, ma, essendo $b(x)$ convergente, possiamo trovare c'' tale che per $|x| \geq c''$ il termine $B_{-h}x^{\frac{h}{k}}$ sia maggiore in modulo di tutto il resto della serie, per cui otteniamo che per $|x| \geq c''$ la serie non si annulla. □

Il risultato fondamentale riguardo alle serie di Puiseux è il seguente

Teorema 2.5 (Newton-Puiseux): Le serie di Puiseux convergenti formano un campo algebricamente chiuso.

Dimostrazione: E' presente in [2], Pagina 279. □

Corollario 2.5.1: Dato un polinomio monico $f(x, T) \in \mathbb{C}[x, T]$ di grado n in x, esistono n serie di Puiseux convergenti

$$x_1(T) = \sum_{i=-h}^{\infty} \frac{B_{1,i}}{T^{\frac{i}{k}}}; \quad x_2(T) = \sum_{i=-h}^{\infty} \frac{B_{2,i}}{T^{\frac{i}{k}}}; \quad \dots ; \quad x_n(T) = \sum_{i=-h}^{\infty} \frac{B_{n,i}}{T^{\frac{i}{k}}} \tag{11}$$

con $B_{j,i} \in \mathbb{C}$, tali che valga l'identità formale

$$f(x, T) = (x - x_1(T))(x - x_2(T))...(x - x_n(T)) \tag{12}$$

e per ogni serie di Puiseux u tale che $f(u(T), T) \equiv 0$, si avrà $u = x_j$ per qualche j.

In particolare, detta τ una radice k-esima di T, possiamo calcolare le serie di Puiseux in τ ed ottenere le serie

$$y_j(\tau) = \sum_{i=-h}^{\infty} \frac{B_{j,i}}{\tau^i}, \tag{13}$$

le quali rispetteranno a loro volta l'identità

$$f(x, T) = (x - y_1(\tau))(x - y_2(\tau))...(x - y_n(\tau)), \tag{14}$$

la quale, fissato T, è un'identità in $\mathbb{C}[x]$.

§ 2.1.i.iii. Un conteggio sui fattori formali —

Ricordiamo che il nostro obiettivo ora è dimostrare Teorema 2.4. Il modo in cui procede la dimostrazione è quello di individuare, in funzione delle serie $x_1, ..., x_n$, quali potrebbero essere i fattori di f in una sua eventuale scomposizione in $\mathbb{Q}[x, T]$.

Definizione 2.1.7: Un fattore formale di $f(x, T)$ è un'espressione della forma

$$\pi_A(x, T) = \prod_{i \in A}(x - x_i) \tag{15}$$

con $A \in S$, e S è l'insieme dei sottoinsiemi propri di $\{1, 2, ..., n\}$.

Questi fattori formali sono interessanti perché se $f(x, T)$ si può scomporre in $\mathbb{Q}[x, T]$, allora i fattori in cui lo scomponiamo devono essere alcuni di questi fattori formali, in particolare f si può scomporre in $\mathbb{Q}[x, T]$ se e solo se esiste un A per cui π_A e π_{A^C} sono entrambi polinomi in $\mathbb{Q}[x, T]$.

Osservazione 2.1.8: Notiamo che un'espressione della forma

$$\prod_{i \in A}(x - x_i(T)) \tag{16}$$

è un polinomio in $\mathbb{Q}[x, T]$ se e solo se le funzioni simmetriche elementari delle $x_i(T)$ con $i \in A$ sono polinomi in $\mathbb{Q}[T]$. Ovvero se e solo se

$$\begin{aligned} x_{i_1} + x_{i_2} + ... + x_{i_{|A|}} &\in \mathbb{Q}[T] \\ &\vdots \\ x_{i_1} x_{i_2} ... \ x_{i_{|A|}} &\in \mathbb{Q}[T]. \end{aligned} \tag{17}$$

In particolare questo accade se queste funzioni simmetriche elementari, viste come serie di Puiseux in T, presentano solo i termini con esponenti di T interi non negativi e se i coefficienti di questi termini sono razionali.

D'ora in poi, quando diciamo di "valutare un fattore formale π_A in t", con $t \in \mathbb{Z}_{>0}$, quello che intendiamo è calcolare il polinomio $\prod_{i \in A}(x - y_i(\tau)) \in \mathbb{C}[x]$, dove τ è la radice k-esima reale positiva di T.

Per trovare qual è il nostro candidato A papabile ad essere il sottonsieme che ci dà la scomposizione di f in $\mathbb{Q}[x, T]$ usiamo l'ipotesi per cui esiste un $t_0 \in \mathbb{Z}$ tale che per $t_1 \geq t_0$ il polinomio $f(x, t_1)$ è riducibile in $\mathbb{Z}[x]$. Sia $t \geq t_0$ un intero.
Ciò significa, per esempio, che almeno uno tra i $\pi_A(x, t)$ al variare di $A \in S$ dovrà essere un polinomio in $\mathbb{Z}[x]$ Analogamente uno tra i $\pi_A\left(x, 2^k t\right)$ al variare di $A \in S$ dovrà essere a coefficienti interi. Lo stesso discorso può essere fatto per i vari $\pi_A\left(x, \sigma^k t\right)$ per ogni $\sigma \in \mathbb{Z}_{>0}$.
Il motivo per cui stiamo specializzando la variabile T a numeri della forma $\sigma^k t$ (e non, ad esempio, a numeri della forma σt) è che in questo modo i τ in cui stiamo calcolando le serie di Puiseux $y_i(\tau)$ formano una progressione aritmetica, il che tornerà utile più avanti.

La prima speranza per trovare il candidato A sarebbe quella di guardare per ogni σ qual è il sottoinsieme di $\{1, ..., n\}$ che ci dà la scomposizione in $\mathbb{Z}[x]$ di $f\left(x, \sigma^k t\right)$ e scegliere uno dei sottoinsiemi che appaiono infinite volte in questa successione (almeno uno deve apparire infinite volte per Pigeonhole).

Purtroppo questo approccio fallisce perché sapere che un fattore formale è a coefficienti interi per infiniti σ non è abbastanza per ricostruire che il fattore formale era un polinomio in $\mathbb{Q}[x, T]$. Ciò che

manca a questo approccio è l'avere della "struttura" su come sono disposti nella progressione aritmetica $1, 2, 3, ...$ i σ per cui un certo coefficiente formale diventa un polinomio in $\mathbb{Z}[x]$.
Quello che il prossimo lemma ci permetterà di fare è trovare un fattore formale π_A e un intero positivo μ_1 tali che, per infiniti σ,

$$\pi_A\big(x, \sigma^k t\big),\ \pi_A\Big(x, (\sigma + \mu_1)^k t\Big) \in \mathbb{Z}[x]. \tag{18}$$

§ 2.1.i.iv. Il Cube Lemma —
Poiché Pigeonhole non era sufficiente a farci ricavare informazioni sui fattori formali, introduciamo un altro lemma combinatorico, più forte, noto come Cube Lemma.

Lemma 2.1.9: (Cube Lemma) Siano dati un intero positivo m e una colorazione di $\mathbb{N}$ con c colori. Allora è possibile trovare m interi positivi $\mu_1, \mu_2, ..., \mu_m$ ed un colore x tra i c della colorazione in modo tale i 2^m numeri della forma

$$\beta + \sum_{i=1}^{m} b_i \mu_i \tag{19}$$

con i b_i uguali a 0 o 1, siano tutti del colore x per infiniti valori di β.

Per dimostrare il Cube Lemma ci serviamo del seguente lemma, sempre riguardante le colorazioni dei naturali.

Lemma 2.1.10: Per ogni coppia di interi positivi m ed c esiste un intero positivo H tale che, per ogni colorazione di $\mathbb{N}$ con c colori ed ogni intervallo I di lunghezza H in $\mathbb{N}$, esistono interi positivi $\beta, \mu_1, ..., \mu_m$ tali che i numeri della forma

$$\beta + \sum_{i=1}^{m} b_i \mu_i \tag{20}$$

con b_i uguali a 0 o 1, siano tutti dello stesso colore e siano tutti all'interno di I.

Dimostrazione: Fissiamo c e dimostriamo la tesi per induzione su m.
Passo base: basta prendere $H = c + 1$ e per Pigeonhole in ogni intervallo lungo $c + 1$ ce ne saranno due dello stesso colore.
Passo induttivo: per ipotesi induttiva esiste un numero h che verifica la tesi per c e $m - 1$.
Sia $H = h\big(1 + c^h\big)$. Dato un intervallo I lungo H partizioniamolo in $1 + c^h$ intervalli lunghi h. Per Pigeonhole ci saranno due di questi intervalli che avranno la stessa colorazione (le colorazioni possibili per un intervallo di lunghezza h sono c^h).
Siano $x, ..., x + (h - 1)$ e $(x + y), ..., (x + y) + (h - 1)$ i due intervalli in questione.
Per ipotesi induttiva nel primo di questi due intervalli possiamo trovare $\beta, \mu_1, ..., \mu_{m-1}$ tali che i numeri $\beta + \sum_{i=1}^{m-1} b_i \mu_i$ abbiano tutti lo stesso colore e stiano nell'intervallo $[x, x + h - 1]$. Ponendo $\mu_m = y$ otteniamo la tesi, poiché i 2^m numeri così ottenuti avranno lo stesso colore, dato che aggiungendo y ai numeri in $[x, x + h - 1]$ otteniamo numeri colorati allo stesso modo. □

Siamo ora pronti per la seguente

Dimostrazione: (Cube Lemma) Sia H il numero della tesi del Lemma 2.1.10. Partizioniamo i numeri naturali negli intervalli $I_j = [jH, (j + 1)H - 1]$ con $j \in \mathbb{N}$. Poiché le possibili colorazioni di un intervallo sono finite, e abbiamo infiniti intervalli, ce ne saranno infiniti colorati allo stesso modo

per Pigeonhole. Siano $I_j, j \in J$ gli intervalli colorati allo stesso modo. Dato uno di questi intervalli, per il Lemma 2.1.10, possiamo trovare $\beta, \mu_1, ..., \mu_m$ tali che i numeri

$$\beta + \sum_{i=1}^{m} b_i \mu_i \tag{21}$$

siano tutti dello stesso colore C. Ma, essendo gli intervalli $I_j, j \in J$ colorati allo stesso modo, in ognuno di essi esisterà un β_j tale che i numeri

$$\beta_j + \sum_{i=1}^{m} b_i \mu_i \tag{22}$$

siano tutti del colore C. □

§ 2.1.i.v. Applicazione del Cube Lemma —

Grazie all'Osservazione 2.1.8 sappiamo che siamo interessati a cercare un insieme A per cui le serie di Puiseux (in cui $i_1, ..., i_{|A|}$ sono gli elementi di A)

$$\begin{aligned} s_1^A &= x_{i_1} + x_{i_2} + ... + x_{i_{|A|}} \\ s_2^A &= x_{i_1}x_{i_2} + x_{i_1}x_{i_3} + ... + x_{i_{|A|-1}}x_{i_{|A|}} \\ &... \\ s_{|A|}^A &= x_{i_1}x_{i_2}... \, x_{i_{|A|}} \end{aligned} \tag{23}$$

siano tutte polinomi in $\mathbb{Q}[T]$.

Riprendendo l'approccio che stavamo seguendo nella Sezione 2.1.i.iii, consideriamo nuovamente i fattori formali della forma $\pi_A\big(x, \sigma^k t\big)$ al variare di $A \in S$ e di $\sigma \in \mathbb{Z}_{>0}$. Sappiamo che per ogni σ c'è un A che rende quel fattore formale un polinomio in $\mathbb{Z}[x]$.
In particolare, un certo A è tale che $\pi_A\big(x, \sigma^k t\big) \in \mathbb{Z}[x]$ se e solo se le serie $s_1^A, ..., s_{|A|}^A$ valutate in $\sigma^k t$ sono dei numeri interi.[1]

Fissato t e detta τ la sua radice k-esima reale positiva, possiamo scriverci le serie $s_i^A\big(\sigma^k t\big)$ come serie di Puiseux ad esponenti interi nella variabile σ (perché τ è fissato), ovvero

$$s_i^A\big(\sigma^k t\big) = \sum_{j=-h_i^A}^{\infty} \frac{c_{i,j}^A}{(\sigma\tau)^j} =: p_i^A(\sigma) \tag{24}$$

Sia $m := \max_{A \in S, 1 \le i \le |A|}\big(h_i^A\big) + 1$.

Ora, immaginiamo di associare ad ogni σ un insieme $A_\sigma \in S$ tale che $\pi_{A_\sigma}\big(x, \sigma^k t\big) \in \mathbb{Z}[x]$. Così stiamo colorando $\mathbb{Z}_{>0}$ con $|S|$ colori, per cui, grazie al Cube Lemma, esistono m interi positivi $\mu_1, \mu_2, ..., \mu_m$, tali che esistano infiniti β per cui gli insiemi

$$A_{\beta + \sum_{j=1}^{m} b_j \mu_j} \tag{25}$$

siano tutti uguali ad un certo insieme A. Sia B l'insieme, infinito, dei β con la proprietà appena descritta.

[1] A priori non è ben definita la valutazione di una serie di Puiseux in un certo punto t, perché compaiono le radici k-esime di un numero, ed ogni numero complesso ne ha k. Però è possibile fissare una radice k-esima di t e sostituire sempre quella a $t^{\frac{1}{k}}$, in questo modo le valuazioni funzionano come al solito.

Dunque sappiamo che per ogni $\beta \in B$ e $(b_1, ..., b_m) \in \{0,1\}^m$, il valore di $p_i^A\left(\beta + \sum_{j=1}^m b_j\mu_j\right)$ è un numero intero. D'ora in poi, poiché è chiaro che stiamo lavorando con l'insieme A, omettiamo l'apice ogni volta che scriviamo p_i^A.

Quello che il Cube Lemma ci permetterà ora di fare è di abbassare il massimo esponente positivo delle serie p_i (quello che indicavamo con h_i^A), fino a che non rimarremo con delle serie composte solo da termini con tutti gli esponenti negativi, le quali, per σ abbastanza grande, dovranno tendere a 0, ma assumendo valori interi per infiniti σ dovranno essere identicamente 0.

§ 2.1.i.vi. Il metodo delle "differenze finite" —

Scriviamo

$$p_i(\sigma) = d_{i,h_i}\sigma^{h_i} + d_{i,h_i-1}\sigma^{h_i-1} + ... + d_{i,0} + \sum_{j=1}^{\infty}\frac{d_{i,-j}}{\sigma^j} \tag{26}$$

e chiamiamo "parte polinomiale" la somma dei termini con esponente non negativo, e "parte negativa" la parte dei termini con esponente negativo, racchiusi nella sommatoria.

Definiamo la serie di Puiseux

$$p_i^{(1)}(\sigma) = p_i(\sigma) - p_i(\sigma + \mu_1) \tag{27}$$

Notiamo che, poiché p_i assumeva valori interi per tutti i numeri della forma $\beta + \sum_{j=1}^m b_j\mu_j$, allora $p_i^{(1)}$ assumerà valori interi per tutti i numeri della forma $\beta + \sum_{j=2}^m b_j\mu_j$.
Notiamo anche che il grado di $p_i^{(1)}$ è sceso rispetto a quello di p_i, perché i termini di grado h_i in $p_i(\sigma)$ e $p_i(\sigma + \mu_1)$ sono entrambi uguali a $d_{i,h_i}\sigma^{h_i}$. Inoltre, vale la seguente

Osservazione 2.1.11: Se la parte negativa di p_i non era identicamente nulla, allora non lo è neanche quella di $p_i^{(1)}$.

Dimostrazione: Naturalmente, quando calcoliamo $p_i^{(1)} = p_i(\sigma) - p_i(\sigma + \mu_1)$, le parti polinomiali si sottraggono tra loro e danno vita alla parte polinomiale di $p_i^{(1)}$, dunque la parte negativa di $p_i^{(1)}$ è data solo dalla differenza tra le parti negative di $p_i(\sigma)$ e $p_i(\sigma + \mu_1)$. Dunque abbiamo (sfruttando il fatto che queste serie sono assolutamente convergenti)

$$\begin{gathered}\sum_{j=1}^{\infty}\frac{d_{i,-j}}{\sigma^j} - \sum_{j=1}^{\infty}\frac{d_{i,-j}}{(\sigma+\mu_1)^j} = \sum_{j=1}^{\infty}\frac{d_{i,-j}}{\sigma^j}\left(1 - \frac{1}{\left(1+\frac{\mu_1}{\sigma}\right)^j}\right) = \\ \sum_{j=1}^{\infty}\frac{\mu_1 j d_{i,-j}}{\sigma^{j+1}}\left(1 - \frac{j+1}{2}\frac{\mu_1}{\sigma} + ...\right)\end{gathered} \tag{28}$$

dove abbiamo espanso $\left(1+\frac{\mu_1}{\sigma}\right)^{-j}$ con i coefficienti binomiali. In particolare, sia l il più piccolo indice per cui $d_{i,-l}$ è non nullo. Allora in $p_i^{(1)}$ tutti i termini con esponenti negativi fino a l (compreso) sono nulli, e il coefficiente di $\sigma^{-(l+1)}$ è $\mu_1 * l * d_{i,-l}$. □

Continuando sulla stessa linea di prima, definiamo anche

$$p_i^{(2)}(\sigma) = p_i^{(1)}(\sigma) - p_i^{(1)}(\sigma + \mu_2) \tag{29}$$

che avrà grado ancora più basso di $p_i^{(1)}$ e anch'essa avrà parte negativa non identicamente nulla, a patto che non lo fosse neanche quella di p_i. Procedendo così possiamo definire $p_i^{(3)}, ..., p_i^{(m)}$ allo stesso modo.

Analogamente a quanto detto per $p_i^{(1)}$, possiamo notare che $p_i^{(m)}(\beta)$ sarà intero per tutti i $\beta \in B$. In particolare, poiché $m \geq h_i$, la parte polinomiale di $p_i^{(m)}$ sarà identicamente nulla, dunque $p_i^{(m)}$ sarà composta solo della parte negativa. Dunque $p_i^{(m)}(\beta)$ è una serie assolutamente convergente composta solo da potenze negative di β, per cui dovrà tendere a 0 per $\beta \to \infty$. Poiché deve anche essere intero, otteniamo che per infiniti β si dovrà avere $p_i^{(m)}(\beta) = 0$. Ma d'altra parte, se calcoliamo il limite

$$\lim_{\beta\to\infty} \beta^{l+m} p_i^{(m)}(\beta) = \mu_1\mu_2...\mu_m l(l+1)...(l+m-1)d_{i,-l} \neq 0 \tag{30}$$

otteniamo un assurdo, per cui la parte negativa di p_i doveva essere identicamente nulla.

§ 2.1.i.vii. p_i è un polinomio a coefficienti razionali in σ —

Poiché abbiamo ottenuto che $p_i(\sigma)$ è un polinomio, esso sarà della forma

$$p_i(\sigma) = d_{i,h_i}\sigma^{h_i} + d_{i,h_i-1}\sigma^{h_i-1} + ... + d_{i,0} \tag{31}$$

Inoltre sappiamo che per infiniti interi positivi σ, $p_i(\sigma)$ è intero. Dunque possiamo scegliere $h_i + 1$ valori diversi di σ e scriverci il sistema

$$\begin{aligned} p_i(\sigma_1) &= d_{i,h_i}\sigma_1^{h_i} + d_{i,h_i-1}\sigma_1^{h_i-1} + ... + d_{i,0} \\ p_i(\sigma_2) &= d_{i,h_i}\sigma_2^{h_i} + d_{i,h_i-1}\sigma_2^{h_i-1} + ... + d_{i,0} \\ &... \\ p_i\big(\sigma_{h_i+1}\big) &= d_{i,h_i}\sigma_{h_i+1}^{h_i} + d_{i,h_i-1}\sigma_{h_i+1}^{h_i-1} + ... + d_{i,0} \end{aligned} \tag{32}$$

che è un sistema di $h_i + 1$ equazioni lineari nelle $h_i + 1$ incognite $d_{i,h_i}, d_{i,h_i-1}, d_{i,0}$. Il determinante della matrice che definisce questo sistema lineare è diverso da 0 perché è il determinante della matrice di Vandermonde dei numeri $\sigma_1, \sigma_2, ..., \sigma_{h_i+1}$. Dunque possiamo risolvere il sistema usando il metodo di Cramer, il quale ci assicura che le soluzioni siano razionali.

§ 2.1.i.viii. s_i^A è un polinomio in $\mathbb{Q}[T]$ —

Da ciò che abbiamo trovato sappiamo che $s_i^A(T)$ è una serie di Puiseux con solo termini con esponente non negativo. Per concludere che è un polinomio ci manca verificare che gli esponenti di T siano tutti interi e che i coefficienti di s_i^A siano razionali (per ora sappiamo che lo sono i coefficienti di p_i). Esplicitiamo meglio la relazione tra s_i^A e p_i. Avevamo

$$s_i^A\big(\sigma^k t\big) = p_i(\sigma) \tag{33}$$

con

$$s_i^A(T) = \sum_{j=0}^{h_i} c_{i,j}^A * T^{\frac{j}{k}}; \quad p_i(\sigma) = \sum_{j=0}^{h_i} \big(c_{i,j}^A \tau^j\big) * \sigma^j. \tag{34}$$

Dunque $s_i^A(T) \in \mathbb{Q}[T]$ se e solo se p_i ha solo termini con esponenti multipli di k. In particolare p_i dipende da t, e se ripercorriamo la dimostrazione notiamo che anche la scelta di quale fattore formale π_A nella Sezione 2.1.i.iii attraverso il Cube Lemma dipendeva da t.

Scegliamo $2^n - 1$ primi distinti $q_1, ..., q_{2^n-1}$, tutti maggiori di t_0. Guardiamo quali fattori formali avremmo scelto tramite il Cube Lemma se avessimo posto $t = q_j$ al variare di $1 \leq j \leq 2^n - 1$. Poiché i possibili fattori formali sono $2^n - 2$ avremo certamente due primi q e q' tali che i fattori formali ottenuti con $t = q$ e $t = q'$ sono gli stessi. Diciamo che il fattore formale ripetuto è quello associato all'insieme $\tilde{A}$.

La cosa interessante è che questo ragionamento ci permette di ottenere due polinomi diversi $p_i(\sigma)$ e $p'_i(\sigma)$, ottenuti tramite le equazioni

$$p_i(\sigma) = s_i^{\tilde{A}}\big(\sigma^k q\big) \tag{35}$$

e

$$p'_i(\sigma) = s_i^{\tilde{A}}\big(\sigma^k q'\big) \tag{36}$$

Entrambi i polinomi così ottenuti, per quanto dimostrato in precedenza, dovranno avere coefficienti razionali. Per quanto scritto nell' Equazione (34) , abbiamo dunque che per ogni $0 \leq j \leq h_i$ i numeri $c_{i,j}^{\tilde{A}} * q^{\frac{j}{k}}$ e $c_{i,j}^{\tilde{A}} * {q'}^{\frac{j}{k}}$ sono razionali. Quindi in particolare nei termini con coefficienti non nulli, ovvero tali che $c_{i,j}^{\tilde{A}} \neq 0$, sarà razionale anche il rapporto $\left(\frac{q}{q'}\right)^{\frac{j}{k}}$, diciamo uguale ad $\frac{a}{b}$ con a e b coprimi. Sia $\frac{c}{d}$ la frazione $\frac{j}{k}$ ridotta ai minimi termini. Dunque abbiamo

$$q^c b^d = {q'}^c a^d \tag{37}$$

in cui q deve dividere a. Sia r il massimo esponente tale che $q^r \mid a$. Affinché i fattori q siano in uguale quantità da entrambe le parti, deve valere $c = dr$, da cui $\frac{j}{k} = \frac{c}{d} \in \mathbb{Z}$ e quindi possiamo concludere che $s_i^{\tilde{A}}(T)$ ha solo potenze con esponente intero. Poiché la relazione tra i coefficienti di $s_i^{\tilde{A}}$ e p_i è

$$c_{i,j}^{\tilde{A}} \tau^j = w_j \tag{38}$$

dove w_j è il coefficiente di σ^j in p_i, e poiché i coefficienti sono non nulli solo per $j = j'k$, allora otteniamo

$$c_{i,j}^{\tilde{A}} \big(\tau^k\big)^{j'} = w_j \tag{39}$$

il che ci garantisce la razionalità di $c_{i,j}^{\tilde{A}}$, poiché $\tau^k = q$ è intero.

Quindi $s_i^{\tilde{A}}$ appartiene a $\mathbb{Q}[T]$ per ogni i, da cui otteniamo che $\pi_{\tilde{A}}(x, T)$ è un polinomio in $\mathbb{Q}[x, T]$ che divide $f(x, T)$.

§ 2.1.ii. Versioni più forti del teorema a due variabili —

Mostriamo ora alcune versioni del teorema di irriducibilità di Hilbert per un polinomio a due variabili, leggermente più forti del Teorema 2.2.

Proposizione 2.1.12: Dato un polinomio irriducibile in 2 variabili $f(x, T) \in \mathbb{Z}[x, T] \setminus \mathbb{Z}[T]$, è possibile sostituire alla variabile T infiniti numeri interi t in modo tale che il polinomio $f(x, t) \in \mathbb{Z}[x]$ sia irriducibile e abbia lo stesso grado di $f(x, T)$ se visto come polinomio in x.

Dimostrazione: Segue immediatamente dal Teorema 2.2 perché i valori di t per cui il grado può scendere sono finiti (se scriviamo $f(x, T) = \sum_{i=0}^{n} f_i(T) x^i$ ci basta richiedere che t non sia radice di $f_n(T)$). Poiché esistono infiniti valori di t ammissibili e ne stiamo escludendo solo finiti, la tesi rimane valida. □

Teorema 2.6: Dati h un polinomi irriducibili in 2 variabili $f_i(x, T) \in \mathbb{Z}[x, T] \setminus \mathbb{Z}[T]$ con $1 \leq i \leq h$, è possibile sostituire alla variabile T infiniti numeri interi t in modo tale che tutti i polinomi $f_i(x, t) \in \mathbb{Z}[x]$ siano contemporaneamente irriducibili e abbiano lo stesso grado dei corrispettivi $f_i(x, T)$.

Dimostrazione: L'affermazione riguardo al far sì che i polinomi $f_i(x,t)$ abbiano lo stesso grado dei polinomi $f_i(x,T)$, come nel caso della proposizione precedente, esclude solo finiti valori di t, per cui ci basta dimostrare il resto del teorema.

La dimostrazione ricalca molto quella del Teorema 2.2, con degli accorgimenti su come usare il Cube Lemma (possiamo dire che sostanzialmente la differenza tra la dimostrazione del Teorema 2.2 e questa è di natura combinatorica).

La contronominale del Teorema 2.6 è: se esiste $t_0 \in \mathbb{Z}$ tale che per ogni $t_1 \geq t_0$ almeno uno degli $f_i(x,t_1)$ si fattorizza in $\mathbb{Z}[x]$, allora uno degli $f_i(x,T)$ è riducibile in $\mathbb{Z}[x,T]$. In maniera del tutto analoga alla Proposizione 2.1.1 possiamo ricondurci ad affrontare il problema nell'ipotesi che gli $f_i(x,t)$ siano monici e vogliamo dimostrare che se esiste $t_0 \in \mathbb{Z}$ tale che per ogni $t_1 \geq t_0$ almeno uno degli $f_i(x,t_1)$ si fattorizza in $\mathbb{Z}[x]$, allora uno degli $f_i(x,T)$ è riducibile in $\mathbb{Q}[x,T]$.

Procediamo in maniera analoga alla dimostrazione del Teorema 2.2 fino all'applicazione del Cube Lemma, ovvero scriviamo per ogni f_i le serie di Puiseux e i suoi fattori formali. Poiché queste serie di Puiseux sono in numero finito, possiamo scriverle tutte nella stessa forma, ovvero possiamo scegliere k, m interi positivi abbastanza grandi tali che tutte le serie si possano scrivere nella forma

$$s(T) = \sum_{j=-m+1}^{\infty} c_j T^{-\frac{j}{k}} \tag{40}$$

Sia W_i l'insieme di tutti i fattori formali di f_i e sia $W = \bigcup_{1\leq i\leq h} W_i$ l'insieme contenente tutti i fattori formali degli f_i. Allora, dato $t \geq t_0$, se guardiamo la successione $\sigma^k t$ con $\sigma \in \mathbb{Z}_{>0}$, abbiamo che per ogni σ dovrà esserci un fattore formale π in W, ovvero un fattore formale di uno degli f_i, tale che $\pi\big(x, \sigma^k t\big) \in \mathbb{Z}[x]$.

Allora coloriamo $\mathbb{Z}_{>0}$ con $|W|$ colori, ognuno associato ad un fattore formale, e per il Cube Lemma possiamo trovare m interi positivi $\mu_1, \mu_2, ..., \mu_m$, tali che esistano infiniti β per cui i numeri

$$\beta + \sum_{j=1}^{m} b_j \mu_j \tag{41}$$

sono tutti associati allo stesso fattore formale.

Procedendo come nella dimostrazione del Teorema 2.2, ora possiamo dimostrare che le serie di Puiseux che determinano i coefficienti di questo fattore formale in funzione di σ non hanno potenze negative di T. Sempre analogamente al Teorema 2.2, possiamo dimostrare che i coefficienti di queste serie di Puiseux sono razionali. Infine, scegliendo $|W|+1$ primi maggiori di t_0 e facendo variare t tra tutti questi primi, ce ne saranno due a cui abbiamo associato lo stesso fattore formale, per cui possiamo fare lo stesso ragionamento della conclusione del Teorema 2.2 per affermare che questo fattore formale è un polinomio in $\mathbb{Q}[x,T]$ e quindi il polinomio f_i di cui questo era un fattore è riducibile in $\mathbb{Q}[x,T]$. □

§ 2.1.iii. Il caso generale —

Vogliamo ora vedere come passare dall'enunciato del teorema di irriducibilità di Hilbert in 2 variabili all'enunciato Teorema 2.1.

Definizione 2.1.13: Dato un campo K chiamiamo specializzazione di Kronecker di grado d in m variabili la mappa

$$\begin{aligned} S_d : K[y_1, ..., y_m] &\to K[z] \\ f(y_1, ..., y_m) &\mapsto f\left(z, z^d, ..., z^{d^{m-1}}\right) \end{aligned} \tag{42}$$

D'ora in poi ometteremo la dipendenza da m, a meno che non specificheremo altrimenti.

Osservazione 2.1.14: La specializzazione di Kronecker dà una bigezione tra

$$K^m_{<d} = \left\{ f \in K[y_1, ..., y_m] |\ \deg_{y_i}(f) < d \forall i \right\} \leftrightarrow \{ f \in K[z] |\ \deg(f) < d^m \} = K_{<d^m} \tag{43}$$

in cui da una parte abbiamo i polinomi in m variabili, di grado minore di d in ognuna di esse, e dall'altra abbiamo i polinomi in una variabile di grado minore di d^m.

Dimostrazione: Segue dall'esistenza e unicità della scrittura in base d. Dato un polinomio in $K^m_{<d}$, è facile notare che la sua specializzazione di Kronecker ha grado minore di d^m. Mentre dato un polinomio in $K_{<d^m}$ possiamo ottenerlo in maniera unica come immagine della specializzazione di Kronecker di un elemento di $K^m_{<d}$ perché il monomio di grado $\sum_{i=0}^{m-1} a_i d^i$ (dove ho scritto un generico grado minore di d^n in base d) si può ottenere solo come immagine del monomio $y_1^{a_1} ... y_m^{a_m}$ o di un suo multiplo scalare. □

Definizione 2.1.15: Un polinomio $f \in K[z]$ si dice d-irriducibile se, per ogni scomposizione $f = gh$ come prodotto di due polinomi non costanti, tali che g e h hanno preimmagini in $K^m_{<d}$, che chiamiamo G e H, allora il prodotto GH non sta in $K^m_{<d}$.

Osservazione 2.1.16: Notiamo che, dato $F \in K^m_{<d}$, se F è riducibile in $K[y_1, ..., y_n]$ allora $S_d(F)$ è d-riducibile. La contronominale ci dice che se $S_d(F)$ è d-irriducibile, allora F è irriducibile.

Dimostrazione: Se F è riducibile sia $F = GH$. Notiamo che i gradi di G, H in ogni variabile dovranno essere minori o uguali a quelli di F, dunque $G, H \in K^m_{<d}$, per cui $S_d(F) = S_d(G)S_d(H)$ è una scomposizione di $S_d(F)$ che lo rende d-riducibile. □

Osservazione 2.1.17: In realtà nell'osservazione precedente vale il se e solo se. Cioè, dato $F \in K^m_{<d}$, F è irriducibile se e solo se $S_d(F)$ è d-irriducibile.

Dimostrazione: Dimostriamo anche la contronominale dell'altra freccia. Se $S_d(F)$ è d-riducibile, allora significa che posso scrivere $S_d(F) = gh$ ed esistono delle preimmagini di g, h in $K^m_{<d}$. Chiamiamole G ed H. Sempre per definizione di d-riducibilità, sappiamo che $F' = GH$ sta in $K^m_{<d}$ e, poiché S_d è omomorfismo, sappiamo che $S_d(F') = S_d(F)$. Allora concludiamo per l'Osservazione 2.1.14. □

Introduciamo ora la seguente proposizione, la quale traccia la strada per l'utilizzo della specializzazione di Kronecker per dimostrare il teorema di Hilbert.

Proposizione 2.1.18: Sia dato $f \in K(x)[z]$ un polinomio d-irriducibile

$$f(x, z) = c_n(x)z^n + ... + c_1(x)z + c_0(x) \tag{44}$$

la cui scomposizione in irriducibili è

$$f = a(x) \prod_{j \in J} p_j(x, z) \tag{45}$$

Se $b \in K$ è tale che i $p_j(b, z)$ sono tutti irriducibili, allora, a parte in un numero finito di eccezioni, $f(b, z)$ è d-irriducibile.

Dimostrazione: A meno di finite eccezioni il coefficiente di testa $a(b)$ è non nullo. Sempre a meno di finite eccezioni il polinomio $p_j(b, z)$ ha lo stesso grado del polinomio $p_j(x, z)$ visto come polinomio in z, e questo vale per ogni j. Dunque possiamo supporre che queste condizioni siano verificate per b. Data una fattorizzazione $f(b, z) = g(z)h(z)$, grazie alle ipotesi di irriducibilità possiamo scrivere

$$g(z) = a_1 \prod_{j \in J_1} p_j(b, z); \quad h(z) = a_2 \prod_{j \in J \setminus J_1} p_j(b, z) \tag{46}$$

con $a_1, a_2 \in K$ tali ch $a_1 a_2 = a(b)$. Definiamo quindi

$$\tilde{g}(x, z) = \frac{a(x)}{a_2} \prod_{j \in J_1} p_j(x, z); \quad \tilde{h}(x, z) = a_2 \prod_{j \in J \setminus J_1} p_j(x, z) \tag{47}$$

Ora, poiché f è d-irriducibile, deve accadere una delle seguenti:

a) Uno tra $\tilde{g}$ e $\tilde{h}$ ha grado (visto come polinomio in z) maggiore o uguale a d^m. In questo caso, dato che siamo nell'ipotesi in cui $\deg_z\big(p_j(b, z)\big) = \deg_z\big(p_j(x, z)\big)$, se $\deg_z(\tilde{g}) \geq d^m$ abbiamo anche $\deg_z(g) \geq d^m$ e lo stesso per h.

b) $\tilde{g}, \tilde{h} \in K(x)_{<d^m}$, in questo caso chiamiamo G e H le loro preimmagini tramite S_d (qui la mappa S_d è intesa tra anelli di polinomi a coefficienti in $K(x)$). Poiché f è d-irriducibile abbiamo $GH \notin K(x)^m_{<d}$, cioè esiste un indice i per cui $\deg_{y_i}(GH) \geq d$. Ma allora scriviamo GH come polinomio in y_i. Il suo coefficiente di testa starà in $K(x)[y_1, ..., y_{i-1}, y_{i+1}, ..., y_m]$ e in particolare sostituendo b a x non potrà diventare identicamente nullo, se non per al massimo un numero finito di valori $b \in K$.
Poiché la specializzazione di Kronecker commuta con la specializzazione della variabile x ad un certo valore b, otteniamo che le preimmagini di g e h tramite S_d (qui la mappa S_d è intesa tra anelli di polinomi a coefficienti in K), che chiameremo G' e H', sono esattamente ciò che otteniamo se in G e H sostituiamo b al posto di x. Dunque in particolare se $\deg_{y_i}(GH) \geq d$, per quanto detto poco sopra varrà anche che $\deg_{y_i}(G'H') \geq d$ a meno di finite eccezioni.

Dunque anche $f(b, z)$ è d-irriducibile. □

Grazie a questa proposizione siamo ora pronti a dimostrare il Teorema 2.1, ovvero il teorema di irriducibilità di Hilbert nel caso in cui specializziamo m variabili.

Proposizione 2.1.19: Il Teorema 2.6 implica il Teorema 2.1.

Dimostrazione: Procediamo per induzione. Per $m = 1$ l'enunciato del Teorema 2.1 è esattamente identico all'enunciato del Teorema 2.2. Procediamo con il passo induttivo. Vogliamo dimostrare che dato un polinomio $f \in \mathbb{Z}[x, T_1, ..., T_m]$ possiamo sostituire a T_m infiniti numeri interi t_m in modo tale che il polinomio $f(x, T_1, ..., T_{m-1}, t_m)$ sia irriducibile in $\mathbb{Z}[x, T_1, ..., T_{m-1}]$. A questo punto ci basterebbe applicare l'ipotesi induttiva per poter sostituire a $T_1, ..., T_{m-1}$ una $(m-1)$-upla di interi $(t_1, ..., t_{m-1})$ in modo tale che il polinomio $f(x, t_1, ..., t_m)$ sia irriducibile in $\mathbb{Z}[x]$.
Dato $f \in \mathbb{Z}[x, T_1, ..., T_m]$, scriviamocelo come $f \in \mathbb{Q}(T_m)[x, T_1, ..., T_{m-1}]$. Sia d un numero inte-

ro positivo più grande del grado complessivo di f. Consideriamo la specializzazione di Kronecker di grado d da $\mathbb{Q}(T_m)[x, T_1, ..., T_{m-1}]$ a $\mathbb{Q}(T_m)[z]$. Notiamo in particolare che $f \in \mathbb{Q}^m_{<d}$ e per l'Osservazione 2.1.17 abbiamo che $S_d(f)$ è d-irriducibile, perché f è irriducibile. Scriviamo

$$S_d(f) = a \prod_{j \in J} p_j(T_m, z) \tag{48}$$

dove, poiché $S_d(f) \in \mathbb{Z}[T_m, z]$, a patto di scegliere bene $a \in \mathbb{Q}$, possiamo supporre che tutti i p_j siano polinomi a coefficienti interi e irriducibili in $\mathbb{Z}[T_m, z]$.
Allora possiamo usare il Teorema 2.6 per trovare infiniti interi b tali che ognuno dei $p_j(b, z)$ sia irriducibile e abbia lo stesso grado del corrispettivo $p_j(x, z)$. Dunque per tutti questi b, tranne al più finiti, grazie alla Proposizione 2.1.18, abbiamo che $S_d(f)(b, z)$ è d-irriducibile, e di conseguenza $f(x, T_1, ..., T_{m-1}, b)$ è irriducibile. □

Concludiamo con la dimostrazione del Corollario 2.1.1.

Dimostrazione (Corollario 2.1.1): Segue da un raffinamento della dimostrazione del Teorema 2.1. Procediamo per induzione. Se $n = 1$, la dimostrazione è analoga a quella della Proposizione 2.1.12. I valori t tali che $a(t)$ sono finiti, dunque anche escludendoli, ci rimangono infiniti valori per cui il polinomio $f(x, t_1) \in \mathbb{Z}[x]$ non sia scomponibile come prodotto di fattori di grado positivo.
Per il passo induttivo, nella dimostrazione di Teorema 2.1 abbiamo dimostrato che, dato $f(\boldsymbol{T}, x)$, possiamo specializzare T_n ad infiniti interi t_n in modo tale che $f(T_1, ..., T_{n-1}, t_n, x)$ sia ancora irriducibile (come prodotto di fattori di grado positivo). Di questi infiniti interi al massimo finiti di essi renderanno il polinomio $a(T_1, ..., T_{n-1}, t_n)$ identicamente nullo, dunque evitando quei valori, tutti gli altri rendono $f(T_1, ..., T_{n-1}, t_n, x)$ irriducibile (come prodotto di fattori di grado positivo) e lasciano il coefficiente di testa non identicamente nullo. Da qui applicando l'ipotesi induttiva possiamo specializzare $T_1, ..., T_{n-1}$ in modo tale che $f(\boldsymbol{t}, x)$ non si scomponga come prodotto di fattori di grado positivo e $a(\boldsymbol{t})$ sia non nullo. □

2.2. Rivestimenti di Galois

Definizione 2.2.1: Una mappa $f : X \to Y$ tra due varietà algebriche X, Y si dice finita se esiste un ricoprimento di Y in aperti affini della forma Spec B_i tali che, dette Spec A_i le rispettive preimmagini e considerando le mappe $g_i : A_i \to B_i$ indotte da f sugli anelli di coordinate, ogni B_i sia un A_i-modulo finitamente generato (B_i assume la struttura di A_i-modulo da g_i, perché possiamo moltiplicare un elemento b di B_i per uno scalare a in A_i tramite $a * b = g_i(a)b$).

Definizione 2.2.2: Chiamiamo rivestimento di Galois, con gruppo G, una mappa (definita su $\mathbb{Q}$) suriettiva e finita tra varietà algebriche definite su $\mathbb{Q}$, $X \to Y$, tale che l'inclusione di campi indotta $\mathbb{Q}(Y) \hookrightarrow \mathbb{Q}(X)$ sia un'estensione di Galois finita con gruppo G.

Osservazione 2.2.3: Un rivestimento in senso classico, ottenuto da un'azione libera e propria di un gruppo G su X dà luogo a un rivestimento di Galois $X \longrightarrow \frac{X}{G}$.

Dimostrazione: L'azione Φ di G su X induce un'azione di G su $\mathbb{Q}(X)$ ($g \in G$ agisce mandando $f \in \mathbb{Q}(X)$ in $f \circ \Phi(g^{-1}) \in \mathbb{Q}(X)$). I punti fissi di $\mathbb{Q}(X)$ per quest'azione sono le funzioni costanti sulle orbite di G in X, ovvero le funzioni definite sul quoziente $\frac{X}{G}$, per cui l'estensione $\mathbb{Q}\left(\frac{X}{G}\right) \hookrightarrow \mathbb{Q}(X)$ è di Galois con gruppo G. □

Notiamo che dato un rivestimento di Galois $X \longrightarrow Y$ con gruppo G (G gruppo finito), possiamo usare il teorema dell'elemento primitivo per trovare un elemento $r \in \mathbb{Q}(X)$ tale che $\mathbb{Q}(X) = \mathbb{Q}(Y)(r)$. Ci mettiamo ora nell'ipotesi in cui $\mathbb{Q}(Y) = \mathbb{Q}(T_1, T_2, ..., T_n)$, dove le T_i sono n variabili indipendenti. La motivazione dietro questa richiesta sta nel fatto che quest'ipotesi ci permette di usare il teorema di irriducibilità di Hilbert, come vedremo a brere.

Chiamiamo $\boldsymbol{T} := (T_1, ..., T_n)$. Indicherò d'ora in poi con le T_i maiuscole le coordinate su Y e con le t_i minuscole una n-upla precisa di numeri razionali, corrispondente alle coordinate di un dato punto in Y.

Sotto quest'ipotesi possiamo scrivere $\mathbb{Q}(X) = \mathbb{Q}(\boldsymbol{T}, r)$ con r radice di un polinomio irriducibile $\tilde{f}(x)$ di grado $k := |G|$ a coefficienti in $\mathbb{Q}(\boldsymbol{T})$. A meno di moltiplicare tutti i coefficienti di $\tilde{f}(x)$ per un denominatore comune, si può vedere $\tilde{f}$ anche come un polinomio in $\mathbb{Z}[T][x]$ o equivalentemente un polinomio $f(\boldsymbol{T}, x)$ a coefficienti in $\mathbb{Z}$. Essendo $\mathbb{Q}(T_1, ..., T_n, r)$ il campo delle funzioni di X, a meno di equivalenza birazionale possiamo immaginare X immerso in $\mathbb{A}^{n+1}$ come la varietà definita dal chiuso di Zariski associato al polinomio $f(\boldsymbol{T}, x)$. In questo modo possiamo usare $(T_1, ..., T_n, r)$ come coordinate su X.

Teorema 2.7: Dato un polinomio $f(T_1, ..., T_n, x) \in \mathbb{Q}[T_1, ..., T_n, x]$ tale che il suo campo di spezzamento su $\mathbb{Q}(T_1, T_2, ..., T_n)$ abbia gruppo di Galois G, è possibile trovare infinite n-uple di numeri razionali $(t_1, t_2, ..., t_n) \in \mathbb{Q}^n$ tali che il campo di spezzamento del polinomio $f(t_1, ..., t_n, x) \in \mathbb{Q}[x]$ abbia gruppo di Galois G su $\mathbb{Q}$.

Per il teorema di irriducibilità di Hilbert, sappiamo che esistono infinite n-uple $\boldsymbol{t} := (t_1, t_2, ..., t_n) \in \mathbb{Z}^n$ tali che il polinomio $f(\boldsymbol{t}, x)$, visto come polinomio nella sola variabile x, sia ancora irriducibile in $\mathbb{Q}[x]$. Sia $a(\boldsymbol{T})$ il coefficiente del termine di grado più alto in x di $f(\boldsymbol{T}, x)$ visto come un polinomio nella variabile x a coefficienti in $\mathbb{Z}[\boldsymbol{T}]$. Naturalmente $a(\boldsymbol{T})$ non può essere identicamente nullo. Dunque per il Corollario 2.1.1 sappiamo che esistono infinite n-uple $\boldsymbol{t} \in \mathbb{Z}^n$ tali che $f(\boldsymbol{t}, x) \in \mathbb{Z}[x]$ sia irriducibile come prodotto di fattori di grado positivo e $a(\boldsymbol{t}) \neq 0$.

Sia P un punto in Y a coordinate $\boldsymbol{t} = (t_1, t_2, ..., t_n)$, tale che $f(\boldsymbol{t}, x)$ sia un polinomio irriducibile in $\mathbb{Q}[x]$ e $a(\boldsymbol{t}) \neq 0$. Allora i punti nella fibra sopra a P saranno k e saranno tutti e soli quelli della forma $Q = (t_1, ..., t_n, \alpha)$ con α una delle k radici del polinomio $f(\boldsymbol{t}, x)$.

Proposizione 2.2.4: Dette $\alpha_1, \alpha_2, ..., \alpha_k \in \overline{\mathbb{Q}}$ le radici di $f(\boldsymbol{t}, x)$, vale $\mathbb{Q}(\alpha_1, ..., \alpha_k) = \mathbb{Q}(\alpha_1)$.

Dimostrazione: Detto Q_i il punto a coordinate $(\boldsymbol{t}, \alpha_i)$, i punti Q_i stanno tutti nella stessa orbita per l'azione di G. Ciò significa che $\forall 1 \leq i \leq k, \exists g_i \in G$ tale che $\Phi(g_i)(Q_1) = Q_i$. Le mappe $\Phi(g_i) : X \to X$ sono tutte mappe algebriche, e in ogni punto sono esprimibili come funzioni razionali, a coefficienti in $\mathbb{Q}$, nelle coordinate. Quindi ogni coordinata di Q_i è esprimibile come funzione razionale delle coordiante di Q_1, e in particolare $\alpha_i \in \mathbb{Q}(\boldsymbol{t}, \alpha_1) = \mathbb{Q}(\alpha_1)$. □

Sia $G' := \mathrm{Gal}(\mathbb{Q}(\alpha_1)/\mathbb{Q})$, che è un estensione di Galois per la proposizione appena dimostrata. Notiamo che $|G'| = k$, perché l'estensione $\mathbb{Q}(\alpha_1)/\mathbb{Q}$ ha grado k, poiché è il grado del polinomio minimo di α_1.

§ 2.2.i. $G' \equiv G$ —

Vogliamo ora dimostrare che $G' \equiv G$. Così facendo avremo dimostrato che l'estensione $\mathbb{Q}(\alpha_1) : \mathbb{Q}$ ha gruppo di Galois G, il che concluderebbe la dimostrazione del Teorema 2.7.

Dimostreremo il seguente teorema:

Teorema 2.8: Dato un polinomio irriducibile $f(T_1, ..., T_n, x) \in \mathbb{Q}[T_1, ..., T_n, x]$ e data una specializzazione $(t_1, ..., t_n) \in \mathbb{Q}^n$ tale che $f(t_1, ..., t_n, x) \in \mathbb{Q}[x]$ sia irriducibile e con lo stesso grado in x di $f(T_1, ..., T_n, x)$, chiamiamo G_i il gruppo di Galois del campo di spezzamento di $f(T_1, ..., T_{n-i}, t_{n-i+1}, ..., t_n, x)$ su $\mathbb{Q}(T_1, ..., T_{n-i})$. Se $|G_0| = |G_n|$, allora $G_0 = G_1 = ... = G_n$.

Sia $\mathbb{L}_1 = \mathbb{Q}(T_1, ..., T_{n-1})$ e consideriamo il dominio di Dedekind $\mathbb{L}_1[T_n]$. Naturalmente il suo campo delle frazioni sarà $\mathbb{L}_1(T_n)$. Possiamo vedere il polinomio $f(\boldsymbol{T}, x)$ come un polinomio a coefficienti in $\mathbb{L}_1$ e nelle variabili (T_n, x), ovvero come polinomio in $\mathbb{L}_1[T_n, x]$. Scriveremo $g(T_n, x)$ per indicare il polinomio appena descritto in $\mathbb{L}_1[T_n, x]$. Consideriamo l'anello $\mathbb{L}_1[T_n, x]/g(T_n, x)$ e sia $\mathbb{F}_1$ il suo campo delle frazioni. In particolare $\mathbb{F}_1 = \mathbb{L}_1(T_n)(\beta)$, dove β è una radice di $f(\boldsymbol{T}, x)$ visto come polinomio in x. Sia inoltre $\mathbb{F}_1'$ la chiusura di Galois di $\mathbb{F}_1 : \mathbb{L}_1(T_n)$ e sia O la chiusura integrale di $\mathbb{L}_1[T_n]$ in $\mathbb{F}_1'$. In particolare notiamo che $G = \mathrm{Gal}(\mathbb{F}_1' : \mathbb{L}_1(T_n))$

Osservazione 2.2.5: A meno di sostituire $\mathbb{L}_1[T_n]$ con la localizzazione per un suo ideale, possiamo assumere che $\mathbb{L}_1[T_n, x]/g(T_n, x) \subseteq O$.

Dimostrazione: Sia $a_1(T_n) \in \mathbb{L}_1[T_n]$ il coefficiente di testa di $g(T_n, x)$ (visto come polinomio in x). Notiamo che, a meno di sostituire $\mathbb{L}_1[T_n]$ con $(a_1(T_n))^{-1}\mathbb{L}_1[T_n]$ (la sua localizzazione in $a_1(T_n)$), possiamo fare in modo che il coefficiente del termine di grado massimo in x sia invertibile. Tutti i risultati che seguono valgono anche se al posto di $\mathbb{L}_1[T_n]$ usiamo la localizzazione appena descritta (in particolare, notiamo che, per come abbiamo scelto la n-upla $t_1, ..., t_n$, abbiamo che $a_1(t_n) \neq 0$), dunque possiamo assumere che il coefficiente di testa di g (visto come polinomio in x) sia invertibile, ovvero, a meno di moltiplicare per uno scalare, che g sia monico. In particolare se g è monico, allora β è intero su $\mathbb{L}_1[T_n]$, e d'altra parte β e le sue potenze generano $\mathbb{L}_1[T_n, x]/g(T_n, x)$. □

Osservazione 2.2.6: Se specializziamo la variabile T_n a t_n (ricordiamo che t_n è l'n-esima coordinata del punto P), notiamo che $g(t_n, x)$ deve avere lo stesso numero di radici distinte di $f(\boldsymbol{T}, x)$, dove stiamo sempre guardando f come polinomio in $\mathbb{Q}(\boldsymbol{T})[x]$.

Dimostrazione: Questo è vero perché abbiamo scelto P in modo che specializzando $\boldsymbol{T}$ a $\boldsymbol{t}$ il numero di radici distinte rimanesse lo stesso, dunque in particolare non può diminuire se specializziamo solo alcune delle variabili T_i. □

§ 2.2.i.i. Richiami di fattorizzazione di primi in estensioni di Galois —

Facciamo ora un breve richiamo di teoria riguardante la fattorizzazione degli ideali primi in estensioni di Galois.

Sia A un dominio di Dedekind con campo delle frazioni K e B la sua chiusura integrale in un'estensione di Galois di K, che chiamiamo K'. Siano p un primo in A e q un primo in B sopra a p.

Il gruppo di Galois di $K' : K$ agisce transitivamente sui primi sopra a p. In particolare tutti i primi sopra a p avranno lo stesso indice di ramificazione e e lo stesso indice di inerzia f. Chiamiamo "gruppo di decomposizione", d'ora in poi indicato con $D(q|p)$, lo stabilizzatore di q in questa azione. Se ci sono r primi distinti sopra a p, allora l'indice $[\mathrm{Gal}(K' : K) : D(q|p)]$ sarà esattamente r, poiché l'indice dello stabilizzatore è pari alla cardinalità dell'orbita. Inoltre, poiché tutti i primi sopra a p hanno indici di ramificazione e di inerzia uguali, vale la formula $[K' : K] = efr$, da cui $|D(q|p)| = ef$.

Vale che l'estensione $B/q : A/p$ è di Galois e ogni elemento di $D(q|p)$ agisce sul quoziente B/q, inducendo così una mappa

$$\varphi : D(q|p) \to \mathrm{Gal}\left(\frac{B}{q} : \frac{A}{p}\right) \tag{49}$$

Chiamiamo "gruppo di inerzia", e indichiamo con $I(q|p)$, il nucleo di questa mappa. Notiamo inoltre che, per definizione di grado di inerzia, $|\mathrm{Gal}\left(\frac{B}{q} : \frac{A}{p}\right)| = f$.

Un importante risultato è dato dal seguente lemma:

Lemma 2.2.7: La mappa

$$\varphi : \frac{D(q|p)}{I(q|p)} \to \mathrm{Gal}\left(\frac{B}{q} : \frac{A}{p}\right) \tag{50}$$

è un isomorfismo. Segue anche che $|I(q|p)| = e$.

Dimostrazione: Nonostante il lemma sia vero in una generalità più ampia, mostriamo una dimostrazione che funziona solo quando $B/q : A/p$ è separabile, il che ai nostri fini non è limitante.
Sia $\overline{\omega}$ un elemento primitivo dell'estensione $B/q : A/p$, ovvero un elemento tale che $B/q = (A/p)(\overline{\omega})$ (tale elemento esiste per il teorema dell'elemento primitivo, e qui stiamo usando il fatto che l'estensione sia separabile). Solleviamo $\overline{\omega}$ ad $\omega \in B$. In particolare, per il teorema cinese del resto, possiamo scegliere $\omega \in B$ in modo tale che $\omega \equiv \overline{\omega}\ (q)$ e $\omega \equiv 0\ (\sigma(q))$ per ogni $\sigma \in \mathrm{Gal}(K' : K) \setminus D(q|p)$. Notiamo che il polinomio

$$h(x) = \prod_{\sigma \in\, \mathrm{Gal}(K':K)} (x - \sigma\omega) \tag{51}$$

è a coefficienti in A, poiché è invariante per l'azione di $\mathrm{Gal}(K' : K)$. Dalla condizione $\omega \equiv 0\ (\sigma(q))$ otteniamo che $\sigma^{-1}(\omega) \equiv 0\ (q)$ per ogni $\sigma \in \mathrm{Gal}(K' : K) \setminus D(q|p)$.
Dunque, proiettando modulo q il polinomio scritto sopra, otteniamo il polinomio

$$\overline{h}(x) = \prod_{\sigma \in D(q|p)} (x - \overline{\sigma\omega}) \ * \prod_{\sigma \in\, \mathrm{Gal}(K':K)\setminus D(q|p)} x \tag{52}$$

che sarà a sua volta a coefficienti in A/p, poiché h era a coefficienti in A.
Ma se $\overline{h}(x)$ è a coefficienti in A/p, allora lo sarà anche il polinomio

$$\tilde{h}(x) = \prod_{\sigma \in D(q|p)} (x - \overline{\sigma\omega}) \tag{53}$$

Dunque le radici coniugate di $\overline{\omega}$ sono tutte della forma $\overline{\sigma\omega}$ con $\sigma \in D(q|p)$. Dunque in particolare $D(q|p)$ agisce transitivamente sulle radici coniugate a $\overline{\omega}$, e, poiché $\overline{\omega}$ genera l'estensione di campi, questo è sufficiente a dire che la mappa nel gruppo di Galois di $(B/q : A/p)$ è suriettiva.

Per un semplice conto degli ordini dei gruppi coinvolti, abbiamo che $\frac{|D|}{|I|} = |\mathrm{Gal}(B/q : A/p)|$, da cui $|I(q|p)| = e$. □

§ 2.2.i.ii. Applicazione al gruppo di Galois della specializzazione —

Ora vogliamo applicare i fatti appena visti al nostro problema. Innanzitutto ci sarà utile dimostrare la seguente:

Proposizione 2.2.8: L'ideale primo $(T_n - t_n)$ di $\mathbb{L}_1[T_n]$ è non ramificato in $\mathbb{F}_1'$.

Dimostrazione: Notiamo che $(T_n - t_n)$ non divide il discriminante di $g(T_n, x)$, perché $g(t_n, x)$ ha k radici distinte, così come $g(T_n, x)$ (visto come polinomio in x). La tesi segue dunque dal prossimo lemma applicato a $A = \mathbb{L}_1[T_n]$. □

Lemma 2.2.9: Dato un primo p in un dominio di Dedekind A, con campo delle frazioni K, e un polinomio monico e separabile $f \in A[x]$, se p è ramificato nel campo di spezzamento di f, allora $p \mid \mathrm{disc}(f)$, dove $\mathrm{disc}(f)$ indica il discriminante del polinomio.

Dimostrazione: Sia K' il campo di spezzamento di f su K e sia B la chiusura integrale di A in K'. Se p è ramificato, significa che, dato un primo q in B, il gruppo di inerzia $I(q|p)$ è non banale. In particolare sia σ un elemento di $I(q|p)$ diverso dall'identità.
Siano $\zeta_1, ..., \zeta_h$ le radici di f (che supponiamo avere grado h). Sia in particolare ζ una radice di f non fissata da σ (ne esisterà necessariamente almeno una, altrimenti σ coinciderebbe con l'identità). Senza perdita di generalità supponiamo $\zeta = \zeta_1$ e $\sigma(\zeta) = \zeta_2$. Possiamo scrivere il discriminante di f come il quadrato del determinante della matrice

$$M = \begin{pmatrix} 1 & \sigma_1(\zeta) & \sigma_1(\zeta^2) & ... & \sigma_1(\zeta^{h-1}) \\ 1 & \sigma_2(\zeta) & \sigma_2(\zeta^2) & ... & \sigma_2(\zeta^{h-1}) \\ \vdots & & & & \\ 1 & \sigma_h(\zeta) & \sigma_h(\zeta^2) & ... & \sigma_h(\zeta^{h-1}) \end{pmatrix} \tag{54}$$

dove $\sigma_1, ..., \sigma_h \in \mathrm{Gal}(K' : K)$ sono elementi del Galois tali che $\sigma_{j(\zeta)} = \zeta_j$. Tali elementi esistono perché l'azione del Galois è transitiva. In questo modo, la matrice che abbiamo scritto non è altro che la matrice di Vandermonde delle radici di f, motivo per cui il suo determinante al quadrato è il discriminante.

In particolare notiamo che possiamo scegliere $\sigma_1 = \mathrm{id}$ e $\sigma_2 = \sigma$.
Guardiamo ora le righe della matrice modulo q. Poiché il gruppo di inerzia agisce banalmente su B/q, ciò significa che la prima e la seconda riga della matrice, che sono

$$\begin{pmatrix} 1 & \zeta & \zeta^2 & ... & \zeta^{h-1} \\ 1 & \sigma(\zeta) & \sigma(\zeta^2) & ... & \sigma(\zeta^{h-1}) \end{pmatrix}, \tag{55}$$

sono uguali nel quoziente per q. Questo in particolare ci dice che la loro differenza sta in q. Poiché il determinante di una matrice è invariante per operazioni elementari di righe e colonne, possiamo calcolare il determinante della matrice M' in cui sostituiamo la prima riga di M con la differenza tra la prima e la seconda riga di M. Così facendo otteniamo una matrice M' che ha una riga composta da tutti elementi in q, per cui il suo determinante, che è uguale a quello di M, starà in q. D'altra parte, se scriviamo il discriminante di f come

$$\mathrm{disc}(f) = \prod_{1 \le i < j \le h} \left(\zeta_i - \zeta_j\right)^2 \tag{56}$$

notiamo che è invariante per l'azione di $\mathrm{Gal}(K' : K)$, per cui sta in K. Ma allora otteniamo che $\mathrm{disc}(f) \in (K \cap q) = (A \cap q) = p$, da cui la tesi. □

Consideriamo quindi il primo $p = (T_n - t_n)$ di $\mathbb{L}_1[T_n]$ e consideriamo un primo q in O che stia sopra a p. Notiamo che, poiché p è non ramificato, ne segue che il gruppo di inerzia $I(q|p)$ è banale. Di conseguenza, il Lemma 2.2.7 ci fornisce un isomorfismo tra $D(q|p)$ e $\mathrm{Gal}(O/q : \mathbb{L}_1[T_n]/p) = \mathrm{Gal}(O/q : \mathbb{L}_1)$.

Di $(O/q : \mathbb{L}_1)$ sappiamo con certezza che è un'estensione di Galois, e sappiamo anche che O/q contiene una radice di $g(t_n, x)$. Questo perché $\beta \in O$ è una radice di $g(T_n, x)$ (visto come polinomio in x) e quando quozientiamo per p questo polinomio diventa $g(t_n, x)$, per cui l'elemento in O/q corrispondente a β sarà una radice di $g(t_n, x)$. Poiché $O/q : \mathbb{L}_1$ è di Galois e contiene una radice di $g(t_n, x)$, otteniamo che O/q dovrà contenere tutto il campo di spezzamento di $g(t_n, x)$.

Dunque si prospettano due scenari:
a) o O/q è esattamente il campo di spezzamento di $g(t_n, x)$ su $\mathbb{L}_1$
b) o O/q contiene strettamente il campo di spezzamento di $g(t_n, x)$ su $\mathbb{L}_1$.

Poiché $D(q|p) = \mathrm{Gal}(O/q : \mathbb{L}_1)$ è immerso in G, vale la seguente disuguaglianza

$$|\mathrm{Gal}(g(t_n, x))| \leq |\mathrm{Gal}(O/q : \mathbb{L}_1)| = |D(q|p)| \leq |G| \tag{57}$$

§ 2.2.i.iii. Iterazione del ragionamento a tutte le n variabili T_i —

Chiamiamo G_i il gruppo di Galois del campo di spezzamento del polinomio $f(T_1, ..., T_{n-i}, t_{n-i+1}, ..., t_n, x)$ su $\mathbb{Q}(T_1, ..., T_{n-i})$. Con questa notazione abbiamo che $G = G_0$ e $G' = G_n$. Il gruppo di Galois di $g(t_n, x)$ su $\mathbb{L}_1$ è G_1.
Siamo ora pronti a dimostrare il Teorema 2.8:

Dimostrazione (Teorema 2.8): L' Equazione (57) ci permette di concludere che $|G_1| \leq |G_0|$. In particolare nel caso b) vale il minore stretto.
D'altra parte, per dire che $|G_i| \leq |G_{i-1}|$, possiamo fare un ragionamento del tutto analogo a quello che abbiamo fatto per dire che $|G_1| \leq |G_0|$. Al posto di usare da $\mathbb{L}_1 = \mathbb{Q}(T_1, ..., T_{n-1})$ usiamo $\mathbb{L}_i = \mathbb{Q}(T_1, ..., T_{n-i})$ e guardiamo l'ideale primo $(T_{n-i+1} - t_{n-i+1})$ nell'anello di Dedekind $\mathbb{L}_i[T_{n-i+1}]$. Il campo $\mathbb{F}_i$ sarà il campo delle frazioni di $\mathbb{L}_i[T_{n-i+1}, x]/f(T_1, ..., T_{n-i+1}, t_{n-i+2}, ..., t_n, x)$, dove f è visto come polinomio in $\mathbb{L}_i[T_{n-i+1}, x]$. In questo caso $\mathbb{F}_i'$ sarà la chiusura di Galois di $\mathbb{F}_i$ su $\mathbb{L}_i(T_{n-i+1})$. Tutti i ragionamenti fatti successivamente funzionano alla stessa maniera e in particolare implicano che $|G_i| \leq |G_{i-1}|$.

Mettendo insieme tutte queste disuguaglianze, otteniamo $|G_n| \leq |G_0|$, ma noi sappiamo già che $|G'| = |G|$, per cui, affinché valga l'uguaglianza, deve valere $|G_i| = |G_{i-1}|$ per ogni i. In particolare questo esclude il caso b).
Riprendendo la notazione dell' Equazione (57) , questo significa che

$$G_1 = \mathrm{Gal}(g(t_n, x)) = \mathrm{Gal}(O/q : \mathbb{L}_1) \equiv D(q|p) \subset G_0 \tag{58}$$

e quindi in particolare G_1 si immerge in G_0, ma avendo la stessa cardinalità otteniamo $G_1 \equiv G_0$. Lo stesso ragionamento si applica in maniera del tutto analoga per dimostrare che $G_i \equiv G_{i-1}$, da cui finalmente segue che $G' \equiv G$. □

sec. 3 — Costruzione del rivestimento per gruppi abeliani

3.1. I tori

La costruzione del rivestimento per i gruppi abeliani utilizza i tori algebrici. Vediamo ora le definizioni e i teoremi rilevanti. Una referenza completa si può trovare in [3].

§ 3.1.i. Nozioni preliminari —

Definizione 3.1.1: Un gruppo algebrico affine è una varietà affine X, dotata di una struttura di gruppo compatibile con la struttura di varietà. Ovvero, X è dotata di una mappa $m : X \times X \to X$ (mappa di moltiplicazione), che chiediamo essere associativa, è dotata di una mappa $i : X \to X$ (mappa dell'inverso), che dev'essere un'involuzione. Inoltre X deve avere un elemento neutro, ovvero deve esistere un punto $e \in X$ tale che

$$m(x, e) = m(e, x) = x,\ \ m(x, i(x)) = e \tag{59}$$

Definizione 3.1.2: L'algebra di Hopf $O(X)$ di un gruppo algebrico affine X è l'anello delle coordinate di X. La mappa di moltiplicazione $m : X \times X \to X$ induce a livello degli anelli di coordinante una mappa, detta mappa di comoltiplicazione, $\Delta : O(X) \to O(X) \otimes O(X)$.

Definizione 3.1.3: Il gruppo algebrico moltiplicativo $\mathbb{G}_m$ è dato dalla varietà algebrica affine definita da $xy = 1$ nel piano $\mathbb{A}^2$, su cui definiamo l'operazione $(x, y) * (x', y') = (xx', yy')$ che è una mappa regolare da $\mathbb{G}_m \times \mathbb{G}_m \longrightarrow \mathbb{G}_m$, e la mappa $(x, y) \mapsto (x^{-1}, y^{-1})$, anch'essa regolare, che associa ad ogni punto il suo inverso. L'elemento neutro è dato dal punto $(1, 1)$.

Osservazione 3.1.4: Notiamo che l'algebra di Hopf di $\mathbb{G}_m$ su $\mathbb{K}$ è $\mathbb{K}[t, t^{-1}]$, dotata della mappa di comoltiplicazione $\Delta : \mathbb{K}[t, t^{-1}] \to \mathbb{K}[t, t^{-1}] \otimes \mathbb{K}[t, t^{-1}]$ indotta da $t \mapsto t \otimes t$.

Definizione 3.1.5: Il gruppo algebrico μ_n è dato dalla varietà algebrica $x^n = 1$ in $\mathbb{A}^1$, con la legge di prodotto $x * x' = xx'$. La sua algebra di Hopf è $O(\mu_n) = \mathbb{K}[T]/(T^n - 1)$ ed eredita la mappa di comoltiplicazione da $O(\mathbb{G}_m)$. Il gruppo $\mu_n\left(\overline{\mathbb{Q}}\right)$ è isomorfo a $\mathbb{Z}/n\mathbb{Z}$.

Definizione 3.1.6: Dato un gruppo G, possiamo creare il gruppo algebrico costante $G_{\mathbb{K}}$, che come varietà algebrica è composta da $|G|$ punti indicizzati sugli elementi di G e il prodotto tra due punti è indotto dal prodotto delle loro indicizzazioni in G. La sua algebra di Hopf è $O(G_{\mathbb{K}}) = \prod_{g \in G} \mathbb{K}_g$, ovvero un prodotto di copie di $\mathbb{K}$, una per ogni punto di $G_{\mathbb{K}}$. Per una descrizione più formale con la teoria degli schemi rimandiamo a [3], Esempio 2.3.

Definizione 3.1.7: Un toro su un campo $\mathbb{K}$ a caratteristica 0 è un gruppo algebrico $\mathbb{T}$ definito su $\mathbb{K}$, tale che $\mathbb{T}_{\overline{\mathbb{K}}}$ (il toro visto come varietà a coefficienti sulla chiusura algebrica) sia isomorfo ad un prodotto finito di copie del gruppo moltiplicativo $\mathbb{G}_m$.

Definizione 3.1.8: Dato un gruppo algebrico H, chiamiamo $X(H)$ il suo gruppo dei caratteri, ovvero il gruppo degli omomorfismi $\chi : H \to \mathbb{G}_m$. Su questo insieme possiamo definire una struttura di gruppo abeliano tramite l'operazione $(\chi + \chi')(h) = \chi(h) * \chi'(h)$.

Osservazione 3.1.9: Notiamo che definire un carattere $\chi : H \to \mathbb{G}_m$ equivale a fornire una mappa di $\mathbb{K}$-algebre $\varphi : O(\mathbb{G}_m) \to O(H)$ che rispetti le mappe di comoltiplicazione. Ovvero tale che il seguente diagramma commuti

$$\begin{array}{ccc} \mathbb{K}[t,t^{-1}] & \xrightarrow{\qquad\varphi\qquad} & O(H) \\ \Big\downarrow{\scriptstyle \Delta_{\mathbb{G}_m}} & & \Big\downarrow{\scriptstyle \Delta_H} \\ \mathbb{K}[t,t^{-1}] \otimes \mathbb{K}[t,t^{-1}] & \xrightarrow{\varphi\otimes\varphi} & O(H)\otimes O(H) \end{array}$$

In particolare una tale mappa è definita univocamente da $\varphi(t)$, e le possibili immagini di t sono tutti e soli gli elementi a di $O(H)$ tali che $\Delta_H(a) = a \otimes a$. Chiameremo "simil-gruppo" gli elementi di $O(H)$ con questa proprietà.
Dunque vi è una corrispondenza tra i caratteri di H e gli elementi simil-gruppo di $O(H)$.

Definizione 3.1.10: Diciamo che un gruppo algebrico H è diagonalizzabile se $O(H)$ è generata dagli elementi simil-gruppo (come $\mathbb{K}$-spazio vettoriale).

Osservazione 3.1.11: Il gruppo $\mathbb{G}_m^n$ è diagonalizzabile.

Dimostrazione: $O(\mathbb{G}_m^n) = \mathbb{K}[t_1, t_1^{-1}, ..., t_n, t_n^{-1}]$ è generata degli elementi della forma $t_1^{l_1} t_2^{l_2} ... t_n^{l_n}$ al variare di $(l_1, l_2, ..., l_n) \in \mathbb{Z}^n$ e ognuno di questi elementi è simil-gruppo. □

Definizione 3.1.12: Chiamiamo $X^*(H)$ il gruppo dei caratteri di $H_{\overline{\mathbb{K}}}$ (con $H_{\overline{\mathbb{K}}}$ indichiamo il gruppo dato dalla varietà su cui è definito H, vista come varietà a coefficienti in $\overline{\mathbb{K}}$). In altri termini

$$X^*(H) := \mathrm{Hom}\Big(H_{\overline{\mathbb{K}}}, \mathbb{G}_{m,\overline{\mathbb{K}}}\Big) \tag{60}$$

In particolare $X^*(-)$ è un funtore controvariante dalla categoria dei gruppi algebrici definiti su $\mathbb{K}$ alla categoria dei gruppi abeliani finitamente generati.

D'ora in poi quando parleremo di caratteri ci riferiremo sempre a questa seconda definizione, se non specificato altrimenti.
Notiamo che il gruppo dei caratteri definiti su $\overline{\mathbb{K}}$ ci interessa particolarmente quando lavoriamo con i tori, perché ci permette di sfruttare la definizione di toro, che è data da un isomorfismo tra il toro visto su $\mathbb{K}$ e un prodotto di copie di $\mathbb{G}_{m,\overline{\mathbb{K}}}$. Infatti vale la seguente

Osservazione 3.1.13: Per un toro $\mathbb{T}$, tale che $\mathbb{T}_{\overline{\mathbb{K}}} \cong \mathbb{G}_{m,\overline{\mathbb{K}}}^n$, vale $X^*(\mathbb{T}) \cong \mathbb{Z}^n$.

Dimostrazione: Notiamo che gli unici omomorfismi $\mathbb{G}_m \to \mathbb{G}_m$ sono quelli della forma $(x, y) \mapsto \big(x^k, y^k\big), k \in \mathbb{Z}$. Questo perché dare un omomorfismo algebrico $\mathbb{G}_m \to \mathbb{G}_m$ equivale a definire due funzioni razionali s_1 e s_2, tali che $(x, y) \mapsto (s_1(x, y), s_2(x, y))$ sia un omomorfismo di gruppi, ovvero tali che $s_i(xx', yy') = s_i(x, y) * s_i(x', y')$. Scrivendo $y = x^{-1}$, notiamo che possiamo scrivere $s_i(x, y) = r_i(x)$ con r funzione razionale in una variabile, con la condizione che $r_i(xx') = r_i(x) * r_i(x')$, da cui è facile concludere che $r_i(x) = cx^k$. Imponendo che $(1, 1) \mapsto (1, 1)$, si ottiene anche

che $c = 1$.
Dunque

$$X^*(\mathbb{T}) = \mathrm{Hom}(\mathbb{G}_m^n, \mathbb{G}_m) = \mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m)^n = \mathbb{Z}^n \tag{61}$$

□

L'obiettivo finale di questa sezione sui tori sarà quello di enunciare un teorema che presenta l'equivalenza tra due categorie, una delle quali è la categoria dei gruppi algebrici di tipo moltiplicativo su $\mathbb{K}$. Vogliamo ora definire questa categoria.

Definizione 3.1.14: Un gruppo algebrico H è detto di tipo moltiplicativo se $H_{\overline{\mathbb{K}}}$ è diagonalizzabile.

Osservazione 3.1.15: I tori sono di tipo moltiplicativo.

Dimostrazione: Segue immediatamente dall'osservazione 4.1.1.3 unita alla definizione di toro. □

Osservazione 3.1.16: Se $\mathbb{K}$ ha caratteristica 0, il gruppo algebrico costante $\mathbb{Z}/n\mathbb{Z}$ è di tipo moltiplicativo.

Dimostrazione: Grazie alla prossima proposizione, abbiamo che ci basta verificare che $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{G}_a) = 0$, ma questo è vero perché $\mathbb{G}_a$ non ha elementi di torsione. □

Proposizione 3.1.17: Un gruppo algebrico H su $\mathbb{K}$ è moltiplicativo se e solo se è commutativo e $\mathrm{Hom}(H, \mathbb{G}_a) = 0$, dove $\mathbb{G}_a$ è il gruppo additivo su $\mathbb{K}$.

Dimostrazione: E' presente in [3], Teorema 14.24. □

§ 3.1.ii. L'azione di $\mathrm{Gal}\left(\overline{\mathbb{K}} : \mathbb{K}\right)$ —

Dato un gruppo algebrico H definito su $\mathbb{K}$, possiamo scrivere gli omomorfismi $H_{\overline{\mathbb{K}}} \to \mathbb{G}_{m,\overline{\mathbb{K}}}$ in coordinate, immergendo H e $\mathbb{G}_m$ in degli spazi affini. Gli omomorfismi in coordinate saranno dati da delle funzioni razionali a coefficienti in $\overline{\mathbb{K}}$. Otteniamo dunque un'azione di $\Gamma := \mathrm{Gal}\left(\overline{\mathbb{K}} : \mathbb{K}\right)$ su $X^*(H)$ data dall'azione su questi coefficienti.

Una definizione equivalente di questa azione, che rende anche evidente il fatto che essa non dipenda da come immergiamo H in uno spazio affine, si può dare tramite l'algebra di Hopf. Se $O(H_{\mathbb{K}})$ è l'algebra di Hopf di H su $\mathbb{K}$, l'algebra di Hopf di $H_{\overline{\mathbb{K}}}$ è data da $O(H_{\overline{\mathbb{K}}}) = O(H_{\mathbb{K}}) \otimes_{\mathbb{K}} \overline{\mathbb{K}}$.
Dunque Γ agisce su $O(H_{\mathbb{K}}) \otimes_{\mathbb{K}} \overline{\mathbb{K}}$ tramite l'azione sulla seconda componente, e l'azione su $O(H_{\overline{\mathbb{K}}})$ induce un'azione su $H_{\overline{\mathbb{K}}}$. L'azione di Γ su $X^*(H)$ è quindi data da

$$\sigma(f) = \sigma_{\mathbb{G}_{m,\overline{\mathbb{K}}}} \circ f \circ \sigma_{H_{\overline{\mathbb{K}}}}^{-1} \tag{62}$$

per ogni $\sigma \in \Gamma$.

E' possibile rendere Γ un gruppo topologico tramite la topologia di Krull. La topologia di un gruppo si può definire esplicitando una base per gli intorni dell'elemento neutro, nel caso della topologia di Krull questa base è data da tutti i sottogruppi di Γ della forma $\mathrm{Gal}\left(\overline{\mathbb{K}} : \mathbb{L}\right)$, dove $\mathbb{L}$ è un'estensione finita di Galois di $\mathbb{K}$.

Diciamo che un'azione di Γ su un insieme S è continua se la mappa $\Gamma \times S \to S$ che definisce l'azione è continua secondo la topologia discreta su S e la topologia prodotto su $\Gamma \times S$.
E' facile notare che un'azione è continua se e solo se $\forall s \in S$ l'insieme $\{\sigma \in \Gamma \mid \sigma(s) = s\}$ è aperto.

In particolare, dalla prima definizione si può notare che ogni omomorfismo $f \in X^*(H)$ è definito su una qualche estensione finita $\mathbb{L}$ di $\mathbb{K}$. Dunque se $\sigma \in \mathrm{Stab}(f)$, allora anche $\sigma * \mathrm{Gal}\big(\overline{\mathbb{K}} : \mathbb{L}\big) \in \mathrm{Stab}(f)$, da cui

$$\mathrm{Stab}(f) = \bigcup_{\sigma \in \mathrm{Stab}(f)} \sigma * \mathrm{Gal}\big(\overline{\mathbb{K}} : \mathbb{L}\big) \tag{63}$$

è aperto in quanto unione di aperti, da cui l'azione di Γ su $X^*(H)$ è continua.

§ 3.1.iii. L'equivalenza di categorie —

Siamo ora pronti ad enunciare i due teoremi principali di questa sezione

Teorema 3.1: Il funtore X è un'equivalenza controvariante dalla categoria dei gruppi algebrici diagonalizzabili alla categoria dei gruppi abeliani finitamente generati. Tramite questa equivalenza, sequenze esatte corte vengono mandate in sequenze esatte corte.

Dimostrazione: La dimostrazione di questo teorema è presente in [3], in cui questo è il teorema 14.9. □

Corollario 3.1.1: In particolare, nell'equivalenza di categorie definita dal Teorema 3.1, i gruppi della forma $\mathbb{G}_m^n$ corrispondono agli $\mathbb{Z}$-moduli liberi, e viceversa.

Dimostrazione: Grazie all'Osservazione 3.1.13 sappiamo che $X(\mathbb{G}_m^n) \cong \mathbb{Z}^n$, ma d'altra parte, essendo un'equivalenza di categorie, se un gruppo algebrico diagonalizzabile H avesse $X(H) \cong \mathbb{Z}^n$, si dovrebbe avere $H \cong \mathbb{G}_m^n$. □

Teorema 3.2: Il funtore X^* è un'equivalenza controvariante dalla categoria dei gruppi algebrici di tipo moltiplicativo su $\mathbb{K}$ alla categoria dei gruppi abeliani finitamente generati dotati di un'azione continua di Γ. Tramite questa equivalenza, sequenze esatte corte vengono mandate in sequenze esatte corte.

Dimostrazione: La dimostrazione di questo teorema è presente in [3], in cui questo è il teorema 14.17. □

Corollario 3.2.1: Nell'equivalenza di categorie definita dal Teorema 3.2, i tori corrispondono agli $\mathbb{Z}$-moduli liberi dotati di un'azione continua di Γ, e viceversa.

Dimostrazione: Dimentichiamoci per un momento dell'azione di Γ. Poiché $X^*(H) = X(H_{\overline{\mathbb{K}}})$, un gruppo di tipo moltiplicativo H corrisponde ad un dato $\mathbb{Z}$-modulo libero tramite l'equivalenza del Teorema 3.2 se e solo se $H_{\overline{\mathbb{K}}}$ corrisponde allo stesso $\mathbb{Z}$-modulo libero tramite l'equivalenza del Teorema 3.1. Si conclude grazie al Corollario 3.1.1. □

Diamo ora un'ultima definizione, che sarà di fondamentale importanza per la costruzione nella prossima sezione

Definizione 3.1.18: Un toro definito su $\mathbb{Q}$ è detto un toro di permutazione se il suo gruppo dei caratteri (su $\overline{\mathbb{Q}}$) ha una base (come $\mathbb{Z}$-modulo) invariante per l'azione di $\mathrm{Gal}\big(\overline{\mathbb{Q}} : \mathbb{Q}\big)$.

3.2. Rivestimenti per gruppi abeliani

Ritornando al problema iniziale, ci chiediamo quando possiamo ottenere un gruppo G come gruppo di Galois di un'estensione $F : \mathbb{Q}(T_1, ..., T_n)$.

Definizione 3.2.1: Un'estensione $F : \mathbb{Q}(T_1, ..., T_n)$ si dice regolare se $F \cap \overline{\mathbb{Q}} = \mathbb{Q}$.

Siamo particolarmente interessati a cercare estensioni di Galois di $\mathbb{Q}(T_1, ..., T_n)$ con gruppo G regolari perché estensioni di questo tipo ci forniscono famiglie infinite di estensioni di Galois di $\mathbb{Q}$ con gruppo G. Vale infatti la seguente proposizione:

Proposizione 3.2.2: Dato un rivestimento di Galois (definito dalla Definizione 2.2.2) $X \to W$, con $W \subset \mathbb{P}^n$ un aperto denso, in cui il campo F delle funzioni razionali di X è un'estensione regolare di $\mathbb{Q}(T_1, ..., T_n)$, tramite la costruzione della Sezione 2.2 è possibile costruire infinite estensioni di Galois di $\mathbb{Q}$ con gruppo G tutte disgiunte tra loro (ovvero tali che l'intersezione tra due qualsiasi di queste sia $\mathbb{Q}$).

Dimostrazione: Una dimostrazione è presente in [1], Corollario 3.3.4. □

Lo stesso non vale per estensioni non regolari. Se ad esempio considerassimo un'estensione $E(T) : \mathbb{Q}(T)$, con E estensione di Galois di $\mathbb{Q}$, questa sarebbe il campo di spezzamento di un certo polinomio $f(x) \in \mathbb{Q}[x]$ su $\mathbb{Q}(T)$. Quindi, quando andiamo a specializzare T, come visto nella Sezione 2.2, queste specializzazioni ci daranno tutte l'estensione $E : \mathbb{Q}$. Poiché siamo interessati a trovare intere famiglie di estensioni di $\mathbb{Q}$ con un certo gruppo di Galois, le estensioni non regolari si rivelano meno interessanti.

Sia data un'estensione regolare di Galois finita $F : \mathbb{Q}(T)$ con gruppo G. Il campo F può essere interpretato geometricamente come il campo delle funzioni di una curva proiettiva liscia C (la curva proiettiva liscia associata al campo, vedi [4], Capitolo 1, Teorema 6.9). In questo contesto, l'estensione di campi $F : \mathbb{Q}(T)$ corrisponde a un rivestimento di Galois $C \to \mathbb{P}^1$ definito su $\mathbb{Q}$, con gruppo G.

Osservazione 3.2.3: Geometricamente, la condizione di regolarità dell'estensione equivale al fatto che C sia assolutamente irriducibile (ovvero la curva C vista su $\overline{\mathbb{Q}}$ è irriducibile).

Dimostrazione: Per dimostrare entrambe le frecce usiamo il fatto che una varietà ridotta è irriducibile se e solo se il suo anello delle funzioni regolari è un dominio, o analogamente se l'anello delle funzioni razionali è un campo (motivo per cui in genere si parla di campo delle funzioni razionali).

Se l'estensione non è regolare, allora sia $\alpha \in \left(F \cap \overline{\mathbb{Q}}\right) \setminus \mathbb{Q}$. Abbiamo che α è una funzione razionale su C, il che equivale al fatto che α sia una funzione regolare su un aperto $U \subset C$. Sia R l'anello delle coordinate di U. L'anello delle coordinate di $U_{\overline{\mathbb{Q}}}$ (la varietà U definita a coefficienti in $\overline{\mathbb{Q}}$) è $R \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$. Ma, poiché $\alpha \in R \cap \overline{\mathbb{Q}}$, allora $\mathbb{Q}[\alpha] \subseteq R \cap \overline{\mathbb{Q}}$ e, poiché α è algebrico, $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$. Sia $B = \mathbb{Q}(\alpha)$. Allora, per la proprietà associativa del prodotto tensore abbiamo

$$R \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} = \left(R \otimes_B \left(B \otimes_{\mathbb{Q}} B\right)\right) \otimes_B \overline{\mathbb{Q}}. \tag{64}$$

Sia $p(x)$ il polinomio minimo di α su $\mathbb{Q}$. Allora

$$B \otimes_{\mathbb{Q}} B = \frac{\mathbb{Q}[x]}{(p(x))} \otimes_{\mathbb{Q}} \mathbb{Q}(\alpha) = \frac{\mathbb{Q}(\alpha)[x]}{(p(x))} \tag{65}$$

in cui possiamo scomporre

$$\frac{\mathbb{Q}(\alpha)[x]}{(p(x))} = \frac{\mathbb{Q}(\alpha)[x]}{(p_1(x))} \times ... \times \frac{\mathbb{Q}(\alpha)[x]}{(p_r(x))} \tag{66}$$

con il teorema cinese del resto, in cui $p_1, ..., p_r$ sono i fattori irriducibili di p in $\mathbb{Q}(\alpha)[x]$. In particolare la scomposizione sarà il prodotto di almeno due campi, perché $(x - \alpha)$ è un fattore non banale di p. Dunque $B \otimes_{\mathbb{Q}} B$ avrà dei divisori di 0 e quando lo tensorizziamo con gli altri anelli rimarranno dei divisori di 0, per cui $R \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ non è un dominio.
D'altra parte, vale il seguente fatto: dato un campo K, se S è una K-algebra ridotta e $K' : K$ è un'estensione separabile, allora $S \otimes_K K'$ è ridotto (dimostrazione presente in [5]). Di conseguenza $R \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ è ridotto.
Allora $U_{\overline{\mathbb{Q}}}$ non è connesso e di conseguenza neanche $C_{\overline{\mathbb{Q}}}$ lo è (un aperto di un connesso è connesso nella topologia di Zariski).

Se l'estensione è regolare usiamo il fatto che se $C_{\mathbb{Q}(\alpha)}$ è irriducibile per ogni estensione finita $\mathbb{Q}(\alpha)$, allora C è assolutamente irriducibile. Infatti se $C_{\overline{\mathbb{Q}}}$ fosse riducibile, ovvero fosse scrivibile come unione di due chiusi propri A_1, A_2, allora consideriamo due punti $P_1 \in (A_1 \setminus A_2), P_2 \in (A_2 \setminus A_1)$ e consideriamo la più piccola estensione K (che sarà finita) in cui giacciono P_1 e P_2, così avremmo che C_K è riducibile.
Per vedere che $C_{\mathbb{Q}(\alpha)}$ è irriducibile, guardiamo l'anello delle coordinate, che è $F \otimes_{\mathbb{Q}} \mathbb{Q}(\alpha)$. Per la proprietà associativa del prodotto tensore abbiamo che

$$F \otimes_{\mathbb{Q}} \mathbb{Q}(\alpha) = F \otimes_{\mathbb{Q}(T)} \big(\mathbb{Q}(T) \otimes_{\mathbb{Q}} \mathbb{Q}(\alpha)\big) \tag{67}$$

e $\mathbb{Q}(T) \otimes_{\mathbb{Q}} \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha)(T)$.
Poiché F è regolare, abbiamo che $F \cap \mathbb{Q}(\alpha)(T) = \mathbb{Q}(T)$. Questo perché, detta K la chiusura di Galois di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$, abbiamo che i sottocampi di $K(T)$ sono in corrispondenza con i sottogruppi di $\mathrm{Gal}(K(T) : \mathbb{Q}(T)) = \mathrm{Gal}(K : \mathbb{Q})$. Il sottogruppo di $\mathrm{Gal}(K : \mathbb{Q})$ che fissa il campo L corrisponde, in $K(T)$ al campo $L(T)$, dunque tutti i sottocampi di $K(T)$ (e quindi anche di $\mathbb{Q}(\alpha)(T)$) sono della forma $L(T)$. D'altra parte F non può contenere nessun campo di questo tipo con $L \neq \mathbb{Q}$, perché altrimenti avremmo $L \subseteq F \cap \overline{\mathbb{Q}}$, il che è assurdo.
Se consideriamo la mappa di moltiplicazione

$$m : F \otimes_{\mathbb{Q}(T)} \mathbb{Q}(\alpha)(T) \to F\mathbb{Q}(\alpha)(T) \subset \overline{\mathbb{Q}(T)} \tag{68}$$

data da

$$a_1 \otimes a_2 \mapsto a_1 a_2 \tag{69}$$

notiamo che è suriettiva ed è una mappa di $\mathbb{Q}(T)$-spazi vettoriali in cui la dimensione dello spazio di partenza e di arrivo è la stessa (è uguale al prodotto dei gradi delle estensioni $F : \mathbb{Q}(T)$ e $\mathbb{Q}(\alpha)(T) : \mathbb{Q}(T)$). Ne segue che è iniettiva, e di conseguenza è un isomorfismo. Quindi il prodotto tensore $F \otimes_{\mathbb{Q}(T)} \mathbb{Q}(\alpha)(T)$ è effettivamente il campo generato da F e $\mathbb{Q}(\alpha)(T)$ all'interno della chiusura algebrica di $\mathbb{Q}(T)$. In particolare è proprio un campo, per cui $C_{\mathbb{Q}(\alpha)}$ è irriducibile. □

Definizione 3.2.4: Diciamo che un rivestimento di Galois $f : X \to Y$ è regolare se X è liscia e assolutamente irriducibile.

Definizione 3.2.5: Diciamo che un gruppo G gode della proprietà Gal_T se esiste un rivestimento regolare $f : C \to \mathbb{P}^1$ con gruppo G.

Osservazione 3.2.6: Definire la proprietà Gal_T solo attraverso i rivestimenti regolari su $\mathbb{P}^1$ non è riduttivo. Data un'estensione regolare di Galois $F : \mathbb{Q}(T_1, ..., T_n)$, possiamo trovare una varietà X assolutamente irriducibile che abbia come campo delle funzioni razionali F. Dall'inclusione $\mathbb{Q}(T_1, ..., T_n) \hookrightarrow F$ possiamo ottenere un rivestimento di Galois di un aperto W di $\mathbb{P}^n$, grazie alla Proposizione 3.2.7. Il Corollario 3.3.1 ci assicura che questo è sufficiente per concludere che, data un'estensione di Galois regolare di $\mathbb{Q}(T_1, ..., T_n)$, ne possiamo ottenere una di $\mathbb{Q}(T)$.

Proposizione 3.2.7: Data un'estensione di Galois $F : \mathbb{Q}(T_1, ..., T_n)$, possiamo trovare una varietà X con campo delle funzioni razionali F e un aperto W di $\mathbb{P}^n$, tali che l'inclusione $\mathbb{Q}(T_1, ..., T_n) \hookrightarrow F$ induca un rivestimento di Galois $X \to W$.

Dimostrazione: Scriviamo $F = \mathbb{Q}(T_1, ..., T_n)(y)$ tramite il teorema dell'elemento primitivo. Sia $\tilde{g}(z) \in \mathbb{Q}(T_1, ..., T_n)[z]$ il polinomio minimo di y. Moltiplicando per i denominatori dei coefficienti di $\tilde{g}$ otteniamo un polinomio $g(z)$ a coefficienti in $\mathbb{Q}[T_1, ..., T_n]$. Possiamo scrivere

$$g = g_m(T_1, ..., T_n)z^m + g_{m-1}(T_1, ..., T_n)z^{m-1} + ... + g_0(T_1, ..., T_n). \tag{70}$$

Sia W l'aperto di $\mathbb{A}^n$ (e quindi anche di $\mathbb{P}^n$) definito da $g_m(T_1, ..., T_n) \neq 0$. Sia

$$X = \{(t_1, ..., t_n, z) \in W \times \mathbb{A}^1 |\ g(t_1, ..., t_n, z) = 0\} \subset W \times \mathbb{A}^1, \tag{71}$$

ovvero l'intersezione del chiuso di $\mathbb{A}^{n+1}$ definito da $g = 0$ e di $W \times \mathbb{A}^1 \subset \mathbb{A}^{n+1}$. Vogliamo dimostrare che $\pi : X \to W$ è un rivestimento di Galois (Definizione 2.2.2). E' evidente che sia suriettivo, dobbiamo verificare che la mappa π sia finita. Riprendendo la Definizione 2.2.1, notiamo che ci è necessario esprimere X e W come unioni di spettri di alcune $\mathbb{Q}$-algebre. Notiamo che $W = \mathrm{Spec}\ \mathbb{Q}[T_1, ..., T_n]\left[\frac{1}{g_m}\right]$, perché $\mathbb{A}^n = \mathrm{Spec}\ \mathbb{Q}[T_1, ..., T_n]$ e W ne è la localizzazione all'aperto in cui g_m è invertibile. Analogamente notiamo che $X = \mathrm{Spec}\ Q[T_1, ..., T_n]\left[\frac{1}{g_m}\right][z]/(g)$ perché $W \times \mathbb{A}^1 = \mathrm{Spec}\ Q[T_1, ..., T_n]\left[\frac{1}{g_m}\right][z]$ e X è il chiuso di $W \times \mathbb{A}^1$ definito da $g = 0$. Allora, come B_i e A_i della Definizione 2.2.1 possiamo usare proprio $\mathbb{Q}[T_1, ..., T_n]\left[\frac{1}{g_m}\right]$ e $Q[T_1, ..., T_n]\left[\frac{1}{g_m}\right][z]/(g)$. Chiamiamo $B = \mathbb{Q}[T_1, ..., T_n]\left[\frac{1}{g_m}\right]$. Ci stiamo chiedendo se $B[z]/(g)$ sia un B-modulo finitamente generato. Ma questo è vero perché è generato dagli elementi $1, z, ..., z^{m-1}$, dato che in $B[z]/(g)$ vale

$$0 = \frac{g(T_1, ..., T_n, z)}{g_m(T_1, ..., T_n)} = z^m + \frac{g_{m-1}(T_1, ..., T_n)}{g_m(T_1, ..., T_n)}z^{m-1} + ... + \frac{g_0(T_1, ..., T_n)}{g_m(T_1, ..., T_n)} \tag{72}$$

e quindi possiamo scrivere tutte le potenze di z con esponenete almeno m in funzione delle potenze di z con esponente tra 0 e $m - 1$. □

Teorema 3.3 (Bertini): Sia X una varietà assolutamente irriducibile e sia $f : X \to W$ un rivestimento di Galois, dove W è un aperto denso di $\mathbb{P}^n$. Allora esiste un aperto di Zariski $U \subseteq \mathrm{Grass}_1(\mathbb{P}^n)$ tale che per ogni $l \in U$ vale che $f^{-1}(l)$ è assolutamente irriducibile (ovvero la retta generica ha preimmagine assolutamente irriducibile).

Dimostrazione: Nel corso della dimostrazione lavoriamo sempre su $\overline{\mathbb{Q}}$, per cui irriducibile in questo contesto significa assolutamente irriducibile nel linguaggio usato finora. Notiamo innanzitutto che possiamo togliere a W un'ipersuperficie B' in modo tale che, detto $A = f^{-1}(W \setminus B')$, la restrizione $f|_A : A \to (W \setminus B')$ sia un rivestimento topologico (non ramificato). Questo è possibile perché,

detto F il campo delle funzioni di X su $\overline{\mathbb{Q}}$, possiamo come nella Sezione 2.2, scrivere $F = \overline{\mathbb{Q}}(W)(r)$ per un certo elemento primitivo r che sarà radice di un polinomio $g(T_0, ..., T_n, x) \in \overline{\mathbb{Q}}(W)[x]$, in cui i coefficienti di g sono rapporti di polinomi in $T_0, ..., T_n$ omogenei dello stesso grado. Allora possiamo, a meno di equivalenza birazionale, sostituire X con la varietà

$$X' = \{(t_0, ..., t_n, x) \in W \times \mathbb{A}^1 \mid g(t_0, ..., t_n, x) = 0\} \subset W \times \mathbb{A}^1 \tag{73}$$

mantenendo l'ipotesi dell'irriducibilità, perché l'equivalenza birazionale conserva l'irriducibilità. Il rivestimento di Galois $X' \to W$ è dato dalla restrizione della proiezione $\pi_1 : W \times \mathbb{A}^1 \to W$ a X'. In particolare il rivestimento è ramificato in un punto $(t_0, ..., t_n) \in W$ se e solo se

$$\operatorname{disc}(g)(t_0, ..., t_n) = 0 \tag{74}$$

che definisce un chiuso, al di fuori del quale il rivestimento è non ramificato. Sia $B = (\mathbb{P}^n \setminus W) \cup B'$. Notiamo che B è un'ipersuperficie tale che $\mathbb{P}^n \setminus B = W \setminus B'$. Sia $g'(t_0, ..., t_n) = 0$ l'equazione polinomiale che definisce $B \subset \mathbb{P}^n$. Notiamo anche che A è denso in X, perché A è aperto e X è irriducibile.

Notiamo che, data una generica retta $l \in \operatorname{Grass}_1(\mathbb{P}^n)$, abbiamo che $f^{-1}(l)$ è irriducibile se e solo se lo è $f^{-1}(l) \cap A$. Questo perché se $f^{-1}(l)$ interseca A, allora $f^{-1}(l) \cap A$ è un aperto denso di $f^{-1}(l)$ e quindi sono birazionalmente equivalenti. Di conseguenza uno è irriducibile solo se lo è l'altro.

Possiamo dunque limitarci a guardare il rivestimento $f|_A : A \to (\mathbb{P}^n \setminus B)$, che è non ramificato. D'ora in poi scriveremo f anche al posto di $f|_A$. Il nostro obiettivo sarà dire che per ogni retta l di $\mathbb{P}^n$ non tangente a B vale che $f^{-1}(l \setminus (l \cap B))$ è connessa (da notare che la retta generica in $\mathbb{P}^n$ non tange B). Poiché $l \setminus (l \cap B)$ è liscia (è isomorfa a una copia di $\mathbb{P}^1$ a cui abbiamo tolto $\deg(g')$ punti), anche la sua preimmagine tramite f (che è un rivestimento) lo è. D'altra parte è noto che una varietà connessa e liscia è irriducibile, per cui

$$f^{-1}(l \setminus (l \cap B)) = f^{-1}(l) \cap A \tag{75}$$

è irriducibile. Grazie alla Proposizione 3.2.8, per dire che $f^{-1}(l \setminus (l \cap B))$ è connessa come varietà algebrica su $\overline{\mathbb{Q}}$, ci basta dimostrare che lo è come varietà analitica su $\mathbb{C}$. Dunque d'ora in poi lavoriamo vedendo le varietà algebriche su $\overline{\mathbb{Q}}$ anche come varietà analitiche su $\mathbb{C}$, dotate della topologia euclidea.

Sia $O \in \mathbb{P}^n \setminus B$. In $\mathbb{P}^n$ possiamo parametrizzare le rette per O naturalmente tramite $\mathbb{P}^{n-1}$, per proiezione da O. Sia $V \subset \mathbb{P}^{n-1}$ l'aperto composto dalle rette per O non tangenti a B.
Ora consideriamo le seguenti due varietà:

$$\begin{aligned} A^* &= \{(x, \lambda) \mid f(x) \in l_\lambda\} \subseteq A \times \mathbb{P}^{n-1} \\ P &= \{(y, \lambda) \mid y \in l_\lambda\} \subseteq (\mathbb{P}^n \setminus B) \times \mathbb{P}^{n-1}. \end{aligned} \tag{76}$$

Notiamo che A^* è birazionalmente equivalente ad A (come varietà algebriche). Infatti per ogni punto $a \in A \setminus f^{-1}(O)$ vi è esattamente un λ per cui $(a, \lambda) \in A^*$, poiché vi è solo una retta passante per $f(a)$ e O. Dunque se consideriamo gli aperti di A^* e A dati da

$$A^* \setminus (f^{-1}(O) \times \mathbb{P}^{n-1}) \quad \text{e} \quad A \setminus f^{-1}(O), \tag{77}$$

questi sono isomorfi tra loro tramite la restrizione della proiezione $\pi_A : A^* \to A$ e sono densi rispettivamente in A^* e A. In particolare, poiché A è irriducibile (come varietà algebrica), anche A^* lo è.
Inoltre notiamo che la mappa $f' = f \times \mathrm{id}$ ci fornisce un rivestimento topologico da A^* in P, perché

f era un rivestimento topologico.
Consideriamo la proiezione $\pi_2 : P \to \mathbb{P}^{n-1}$. Ogni retta che non tange B interseca B in esattamente $\deg(g')$ punti per il teorema di Bezout, dunque la fibra sopra ad ogni punto λ in V è data da un $\mathbb{P}^1$ (la retta in $\mathbb{P}^n$ indicizzata da λ) a cui sono stati sottratti $\deg(g')$ punti. In particolare, come varietà analitiche complesse, queste sono tutte isomorfe a delle sfere a cui è tolto un numero finito di punti e quindi sono connesse. Mettendosi in un'opportuna carta complessa, è possibile dimostrare che, dato un aperto $\tilde{U} \subset V$ è possibile costruire un isomorfismo tra $\tilde{U} \times \left(\mathbb{P}^1 \setminus \left\{Q_1, ..., Q_{\deg(g')}\right\}\right)$ (dove $Q_1, ..., Q_{\deg(g')}$ sono dei punti fissati su $\mathbb{P}^1$) e $\pi_2^{-1}\left(\tilde{U}\right)$ tale che il diagramma

$$\begin{array}{ccc} \tilde{U} \times \left(\mathbb{P}^1 \setminus \left\{Q_1, ..., Q_{\deg(g')}\right\}\right) & \overset{\Phi}{\to} & \pi_2^{-1}\left(\tilde{U}\right) \\ \Big\downarrow{\scriptstyle \mathrm{pr}_1} & \swarrow{\scriptstyle \pi_2} & \\ V & & \end{array}$$

commuti (intuitivamente è possibile perché i $\deg(g')$ punti di intersezione di una certa retta con B si spostano in maniera continua se muoviamo di poco la retta e, grazie al fatto che stiamo considerando rette non tangenti a B è possibile, con il teorema della funzione implicita, trovare $\deg(g')$ funzioni che associano ad ogni retta i suoi punti da rimuovere). Dunque la mappa $\pi_2 : P \to \mathbb{P}^{n-1}$ ristretta a V è un fibrato.
Sia $h = \pi_2 \circ f' : A^* \to \mathbb{P}^{n-1}$. La composizione di due fibrati è un fibrato, dunque, poiché $f' : A^* \to P$ è un rivestimento e $\pi_2 : P \to \mathbb{P}^{n-1}$ sopra a V è un fibrato, allora anche h è un fibrato sopra a V. Notiamo che $h^{-1}(V)$ è irriducibile (algebricamente), perché è aperto (è preimmagine di V) in A^*, che è irriducibile. Inoltre V è liscio, per cui anche la sua preimmagine $h^{-1}(V)$ è liscia. Ne segue che $h^{-1}(V)$ è connesso algebricamente e, per la Proposizione 3.2.8 lo è anche come varietà complessa. Analogamente V è aperto di $\mathbb{P}^{n-1}$, che è irriducibile, ed è liscio, per cui è connesso algebricamente, e per la Proposizione 3.2.8 anche analiticamente.
Notiamo che dato $O' \in f^{-1}(O)$, possiamo costruire una sezione per la mappa h data da $\lambda \mapsto (O', \lambda)$.

Dunque la mappa $h : h^{-1}(V) \to V$ è un fibrato (in senso topologico classico) tra due spazi connessi che ammette una sezione. Vogliamo dimostrare che la fibra deve necessariamente essere connessa. Se la fibra F fosse sconnessa consideriamone una sua scomposizione in due aperti disgiunti U_1 e U_2. Dato un aperto trivializzante $\tilde{U} \subset V$, ovvero tale che esista un isomorfismo

$$\begin{array}{ccc} \tilde{U} \times F & \xrightarrow{\Psi_{\tilde{U}}} & h^{-1}\left(\tilde{U}\right) \\ \Big\downarrow{\scriptstyle \pi_1} & \swarrow{\scriptstyle h} & \\ V & & \end{array}$$

abbiamo che possiamo scrivere $h^{-1}\left(\tilde{U}\right) \equiv \tilde{U} \times (U_1 \sqcup U_2) = \left(\tilde{U} \times U_1\right) \sqcup \left(\tilde{U} \times U_2\right)$. In particolare possiamo scegliere $\tilde{U}$ connesso (dato $\tilde{U}$ non connesso, una sua componente connessa dovrà essere aperta in $\tilde{U}$ e di conseguenza in V, dunque possiamo restringerci a quella componente connessa,

che sarà a sua volta trivializzante). Essendo $\tilde{U}$ connesso, la sua immagine tramite la sezione sarà connessa a sua volta e quindi sarà contenuta in solo una delle due componenti aperte disgiunte $\tilde{U} \times U_1$ e $\tilde{U} \times U_2$. Chiamiamo tale componente $c_1\big(\tilde{U}\big)$ e chiamiamo l'altra componente aperta $c_2\big(\tilde{U}\big)$. Consideriamo

$$C_i = \bigcup_{\tilde{U} \subseteq V,\ \tilde{U} \text{ trivializ.}} c_i\big(\tilde{U}\big) \tag{78}$$

e notiamo che sia C_1 sia C_2 sono aperti, sono disgiunti e la loro unione dà tutto $h^{-1}(V)$, da cui l'assurdo.

Dunque la fibra di $\lambda \in V$, che è esattamente $f^{-1}(l_\lambda \setminus (l_\lambda \cap B))$, è connessa.

□

Corollario 3.3.1: Dato un rivestimento regolare con gruppo G su un aperto denso W di $\mathbb{P}^n$ ne possiamo costruire uno su $\mathbb{P}^1$. In particolare, data un'estensione di Galois regolare di $\mathbb{Q}(T_1, ..., T_n)$ con gruppo G, ne possiamo ottenere una di $\mathbb{Q}(T)$.

Dimostrazione: Dato un rivestimento di Galois regolare $f : X \to W$, scegliamo una retta generica l in $\mathbb{P}^n$. Per Teorema 3.3 sappiamo che $Y = f^{-1}(l) = f^{-1}(l \cap W)$ è assolutamente irriducibile.
Se consideriamo la mappa $f|_Y : Y \to (l \cap W)$ (in cui $l \cap W$ è un aperto denso di $\mathbb{P}^1$) notiamo che essa sarà a sua volta un rivestimento di Galois perché $f|_Y$ è suriettiva, dato che lo era f. Inoltre il gruppo G agiva su X generando il rivestimento ramificato, ma l'azione di G è chiusa per fibre, quindi si può restringere ad un'azione su Y, la quale induce $f|_Y$. Inoltre è sempre possibile trovare una curva proiettiva liscia Y' birazionalmente equivalente a Y ([4], Capitolo 1, Corollario 6.11). Notiamo che la mappa $\varphi : Y' \to \mathbb{P}^1$ indotta dal'inclusione di campi $\mathbb{Q}(T) \hookrightarrow \mathbb{Q}(Y')$ è suriettiva. Questo perché l'immagine di una varietà proiettiva è chiusa (vedi [6], Sezione 5.2, Teorema 1.10) e, poiché Y' è connessa (è liscia ed irriducibile), l'immagine dovrà essere a sua volta connessa. Gli unici sottoinsiemi non vuoti, chiusi e connessi di $\mathbb{P}^1$ sono i singoli punti e tutto $\mathbb{P}^1$. Essendo φ non costate, l'immagine dovrà essere tutto $\mathbb{P}^1$. Dunque Y' è liscia, assolutamente irriducibile e ci dà un riverstimento di Galois regolare su $\mathbb{P}^1$. □

Nella dimostrazione del Teorema 3.3 abbiamo usato la seguente proposizione:

Proposizione 3.2.8: Sia X una varietà algebrica su $K \subseteq \mathbb{C}$ tale che la varietà analitica $X(\mathbb{C})$ data dai punti complessi di X sia connessa (secondo la topologia di varietà complessa). Allora X è connessa come varietà algebrica su K, ovvero secondo la topologia di Zariski.

Dimostrazione: Dimostreremo solo che se $X(\mathbb{C})$ è connessa come varietà analitica allora anche X è connessa come varietà algebrica. Per l'altra freccia rimandiamo a [7], Proposizione 2.5.

Dimostriamo la contronominale. Se X fosse sconnessa come varietà algebrica, allora esisterebbero due aperti di Zariski U_1, U_2 disgiunti e tali che $U_1 \cup U_2 = X$. Se guardiamo questi due aperti nella varietà analitica $X(\mathbb{C})$, essi sarannno ancora aperti perché la topologia euclidea è più fine di quella di Zariski, per cui questo ci dà la sconnessione della varietà analitica. □

§ 3.2.i. Il prodotto di gruppi —

Vogliamo ora dimostrare che se due gruppi G_1 e G_2 hanno la proprietà Gal_T, ovvero ammettono un rivestimento regolare su $\mathbb{P}^1$, allora anche il loro prodotto $G_1 \times G_2$ ha la medesima proprietà.

Per dimostrarlo sarà fondamentale il prossimo lemma. Diamo prima una definizione preliminare:

Definizione 3.2.9: Una varietà algebrica Y si dice algebricamente semplicemente connessa se ogni rivestimento non ramificato $X \to Y$ è banale, cioè X è l'unione disgiunta di un numero finito di copie di Y.

Lemma 3.2.10: $\mathbb{P}^1$ è algebricamente semplicemente connesso.

Dimostrazione: [4] Capitolo 4, Esempio 2.5.3. □

Dopo questo lemma, possiamo ora dimostrare la seguente proposizione:

Proposizione 3.2.11: Se due gruppi G_1 e G_2 hanno la proprietà Gal_T, allora anche il loro prodotto $G_1 \times G_2$ ce l'ha.

Dimostrazione: Siano $f_1 : C_1 \to \mathbb{P}^1$ e $f_2 : C_2 \to \mathbb{P}^1$ i rivestimenti regolari per G_1 e G_2, e siano Σ_1, Σ_2 gli insiemi dei punti di ramificazione di f_1, f_2 su $\mathbb{P}^1$. Notiamo che Σ_1 e Σ_2 hanno cardinalità finita. Questo perché abbiamo dimostrato che il luogo dei punti di ramificazione è un chiuso e i chiusi non banali di $\mathbb{P}^1$ sono discreti. Di conseguenza, possiamo assumere che $\Sigma_1 \cap \Sigma_2 = \emptyset$, perché se così non fosse potremmo comporre f_2 con un automorfismo di $\mathbb{P}^1$, in modo tale da spostare Σ_2 e renderlo disgiunto da Σ_1 (il che è possibile perché entrambi gli insiemi sono finiti).

Allora le estensioni di campi $\mathbb{Q}(C_1) : \mathbb{Q}(T)$ e $\mathbb{Q}(C_2) : \mathbb{Q}(T)$ sono linearmente disgiunte. Questo perché, detto $K = \mathbb{Q}(C_1) \cap \mathbb{Q}(C_2)$, abbiamo che K è a sua volta il campo delle funzioni di una curva assolutamente irriducibile C', la quale ci dà un rivestimento regolare $f' : C' \to \mathbb{P}^1$. Poiché l'inclusione di campi $\mathbb{Q}(T) \hookrightarrow \mathbb{Q}(C_i)$ si può fattorizzare tramite l'inclusione in $\mathbb{Q}(C')$, allora i rivestimenti f_i si possono fattorizzare tramite delle mappe $C_i \to C'$ composte con f'. In particolare, poiché l'indice di ramificazione è moltiplicativo, per ogni $P \in \mathbb{P}^1$ vale $e_{P,f'} \mid e_{P,f_i}$. Ma, dato che $\Sigma_1 \cap \Sigma_2 = \emptyset$, sappiamo che, per ogni P, almeno uno tra e_{P,f_1} e e_{P,f_2} è uguale a 1, da cui otteniamo che f' è un rivestimento non ramificato. Poiché $\mathbb{P}^1$ è algebricamente semplicemente connesso, deduciamo che $C' = \mathbb{P}^1$ e quindi $\mathbb{Q}(C_1) \cap \mathbb{Q}(C_2) = K = \mathbb{Q}(T)$.

Consideriamo il prodotto fibrato $C = C_1 \times_{\mathbb{P}^1} C_2$, definito come

$$C_1 \times_{\mathbb{P}^1} C_2 = \{(x_1, x_2) \in C_1 \times C_2 \mid f_1(x_1) = f_2(x_2)\} \subset C_1 \times C_2. \tag{79}$$

Grazie alla Proposizione 3.2.12, sappiamo che il campo delle funzioni di $C_1 \times_{\mathbb{P}^1} C_2$ è $\mathbb{Q}(C) = \mathbb{Q}(C_1) \otimes_{\mathbb{Q}(T)} \mathbb{Q}(C_2)$. Vi è una mappa naturale dal prodotto fibrato in $\mathbb{P}^1$, data dal seguente diagramma

$$\begin{array}{ccc} C_1 \times_{\mathbb{P}^1} C_2 & \xrightarrow{\pi_1} & C_1 \\ \downarrow{\scriptstyle \pi_2} & & \downarrow{\scriptstyle f_1} \\ C_2 & \xrightarrow{f_2} & \mathbb{P}^1 \end{array}$$

Questa mappa ci fornisce un rivestimento $C_1 \times_{\mathbb{P}^1} C_2 \to \mathbb{P}^1$. Poiché $\mathbb{Q}(C_1) \cap \mathbb{Q}(C_2) = \mathbb{Q}(T)$, notiamo che il gruppo $G_1 \times G_2$ agisce sul campo $\mathbb{Q}(C_1) \otimes_{\mathbb{Q}(T)} \mathbb{Q}(C_2)$ tramite l'azione in cui G_1 agisce

sulla prima coordinata e G_2 sulla seconda. I punti fissi di quest'azione sono solo gli elementi di $\mathbb{Q}(T)$, e quindi $G_1 \times G_2$ è il gruppo di Galois di $\Big(\mathbb{Q}(C_1) \otimes_{\mathbb{Q}(T)} \mathbb{Q}(C_2)\Big) : \mathbb{Q}(T)$. □

Proposizione 3.2.12: Dati due rivestimenti di Galois $f_1 : C_1 \to \mathbb{P}^1$ e $f_2 : C_2 \to \mathbb{P}^1$ come sopra, tali che $\mathbb{Q}(C_1) \cap \mathbb{Q}(C_2) = \mathbb{Q}(T)$, il campo delle funzioni del prodotto fibrato $C = C_1 \times_{\mathbb{P}^1} C_2$ è $\mathbb{Q}(C) = \mathbb{Q}(C_1) \otimes_{\mathbb{Q}(T)} \mathbb{Q}(C_2)$.

Dimostrazione: Utilizziamo il seguente fatto:

Le funzioni regolari di un prodotto fibrato $X \times_Z Y$ dove X è una varietà e la mappa $Y \to Z$ è piatta sono $O(X) \otimes_{O(Z)} O(Y)$. Questo fatto noto è dimostrato in [8], Punto (2).

Nel nostro caso entrambe le mappe f_1 e f_2 sono piatte perché sono mappe finite tra curve lisce (questo che stiamo usando noi è una versione più debole di [9], Teorema 26.2.11). Consideriamo $\mathbb{A}^1 \subset \mathbb{P}^1$ e siano U_1 e U_2 due aperti affini contenuti nelle preimmagini tramite f_1 e f_2 di $\mathbb{A}^1$. In particolare, poiché C_1, C_2 sono irriducibili, anche U_1, U_2 lo sono, quindi gli anelli delle funzioni regolari $O(U_1)$ e $O(U_2)$ sono dei domini.

Notiamo che $U = U_1 \times_{\mathbb{A}^1} U_2$ è un aperto di C. Poiché è aperto, il suo campo delle funzioni razionali è lo stesso di C (sono birazionalmente equivalenti). Grazie al fatto riportato sopra, sappiamo che

$$O(U) = O(U_1) \otimes_{O(\mathbb{A}^1)} O(U_2) = O(U_1) \otimes_{\mathbb{Q}[T]} O(U_2). \tag{80}$$

D'altra parte, detto $F_i \subset \overline{\mathbb{Q}(T)}$ il campo delle funzioni razionali di U_i, consideriamo la mappa di moltiplicazione

$$m : F_1 \otimes_{\mathbb{Q}(T)} F_2 \to F_1 F_2 \subset \overline{\mathbb{Q}(T)} \tag{81}$$

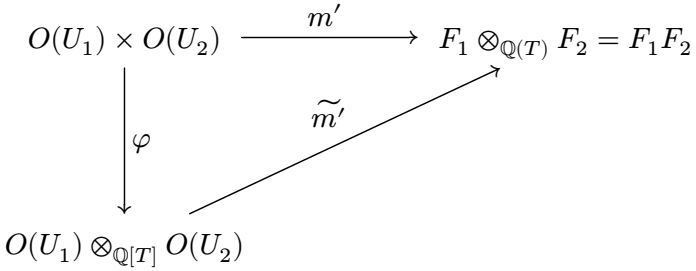
data da

$$a_1 \otimes a_2 \mapsto a_1 a_2 \tag{82}$$

e notiamo che è suriettiva, ma è anche una mappa di $\mathbb{Q}(T)$-spazi vettoriali in cui la dimensione dello spazio di partenza e di arrivo è la stessa ed è uguale al prodotto dei gradi delle estensioni $(F_i : \mathbb{Q}(T))$ (per lo spazio $F_1 F_2$ questo è vero perchè $F_1 \cap F_2 = \mathbb{Q}(T)$). Dunque è anche iniettiva e quindi è un isomorfismo.
Inoltre vi è un'immersione naturale

$$O(U_1) \otimes_{\mathbb{Q}[T]} O(U_2) \hookrightarrow F_1 \otimes_{\mathbb{Q}(T)} F_2 \tag{83}$$

data dalla proprietà universale del prodotto tensore, ovvero che fa commutare il diagramma



in cui $m'(a_1 \otimes a_2) = a_1 a_2$ è la mappa data dalla moltiplicazione e la mappa $\widetilde{m'}$ è iniettiva perché $O(U_1) \cap O(U_2) = \mathbb{Q}[T]$ (possiamo prendere una $\mathbb{Q}[T]$-base di $O(U_1) \otimes_{\mathbb{Q}[T]} O(U_2)$ e vedere che gli elementi della base vanno in elementi in F_1F_2 linearmente indipendenti su $\mathbb{Q}(T)$).

Quindi in particolare $O(U_1) \otimes_{\mathbb{Q}[T]} O(U_2)$ sarà un dominio e, poiché $F_1 \otimes_{\mathbb{Q}(T)} F_2$ è un campo, varrà $\mathrm{Frac}(O(U)) \subseteq F_1 \otimes_{\mathbb{Q}(T)} F_2$. D'altra parte, le proiezioni π_1 e π_2 date dal diagramma

$$\begin{array}{ccc} U_1 \times_{\mathbb{A}^1} U_2 & \xrightarrow{\pi_1} & U_1 \\ \downarrow{\scriptstyle \pi_2} & & \downarrow{\scriptstyle f_1} \\ U_2 & \xrightarrow{f_2} & \mathbb{A}^1 \end{array}$$

definiscono delle inclusioni di F_1 e F_2 in $\mathrm{Frac}(O(U))$, e quindi definiscono anche un'inclusione di F_1F_2 in $\mathrm{Frac}(O(U))$, da cui l'isomorfismo desiderato.

□

§ 3.2.ii. Costruzione tramite i tori —

Sia G un gruppo abeliano finito. Poiché ogni gruppo abeliano finito è la somma diretta di gruppi ciclici, grazie alla Proposizione 3.2.11 possiamo limitarci a considerare G un gruppo ciclico finito di ordine n.
Sia $\Gamma_{\mathbb{Q}} = \mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$.
Vogliamo costruire il rivestimento regolare per il gruppo G mettendo insieme i risultati dei seguenti due teoremi:

Teorema 3.4: Dato G abeliano finito, esiste un toro algebrico S su $\mathbb{Q}$, e un'immersione di G in $S(\mathbb{Q})$ (i punti $\mathbb{Q}$-razionali di S), tale che il quoziente $S' = S/G$ sia un toro di permutazione.

Teorema 3.5: Dato un toro di permutazione S' di rango n, il suo campo delle funzioni è $\mathbb{Q}(T_1, ..., T_n)$.

Inoltre, se S' è il quoziente di un toro S per l'azione di un gruppo finito G (come nell'enunciato del Teorema 3.4), l'estensione $\mathbb{Q}(S) : \mathbb{Q}(S')$ è regolare.

§ 3.2.ii.i. Costruzione della succesione esatta —

Trovare S, S' che soddisfino la prima proposizione, significa costruire una sequenza esatta corta della forma

$$1 \to G \to S \to S' \to 1 \tag{84}$$

L'idea chiave per trovare una sequenza di questo tipo è sfruttare il Teorema 3.2, il quale ci dice che se applichiamo il funtore X^* a tutti i termini della sequenza, la sequenza che troveremo sarà esatta se e solo se quella di partenza lo era.

Osservazione 3.2.13: Per poter applicare il funtore X^*, dobbiamo dotare G di una struttura di gruppo algebrico. Questo è possibile perché possiamo dotare G della struttura di gruppo algebrico costante, secondo la Definizione 3.1.6. In questo modo G è di tipo moltiplicativo grazie alla Osservazione 3.1.16.

Utilizzare X^* ci permette di spostare il problema sugli $\mathbb{Z}\big[\Gamma_{\mathbb{Q}}\big]$-moduli e lavorare con essi anziché lavorare con i gruppi algebrici della sequenza scritta sopra. Siamo quindi interessati a trovare una sequenza di $\mathbb{Z}\big[\Gamma_{\mathbb{Q}}\big]$-moduli della forma

$$0 \to M' \to M \to X^*(G) \to 0 \tag{85}$$

in cui i moduli M e M' sono soggetti a dei vincoli dovuti al fatto che devono essere l'immagine tramite X^* di S e S'. In particolare l'unica condizione su M è che sia uno $\mathbb{Z}$-modulo libero, grazie al Corollario 3.2.1, mentre M' deve essere anch'esso uno $\mathbb{Z}$-modulo libero e deve avere una $\mathbb{Z}$-base invariante per l'azione di $\Gamma_{\mathbb{Q}}$.

Per proseguire vogliamo capire che $\mathbb{Z}\big[\Gamma_{\mathbb{Q}}\big]$-modulo è $X^*(G)$.

Osservazione 3.2.14: $X^*(G) = \mathrm{Hom}_{\overline{\mathbb{Q}}}(G, \mathbb{G}_m) \cong \mathbb{Z}/n\mathbb{Z}$ come $\mathbb{Z}$-modulo

Dimostrazione: Scelto un generatore g di G, un omomorfismo è univocamente determinato dall'immagine di g. Dunque il gruppo degli omomorfismi è isomorfo al gruppo delle immagini di g, che sono esattamente le radici n-esime dell'unità. □

Osservazione 3.2.15: Come $\mathbb{Z}\big[\Gamma_{\mathbb{Q}}\big]$-modulo (ovvero come gruppo abeliano con un'azione di $\Gamma_{\mathbb{Q}}$), $X^*(G)$ è isomorfo a $\mu_{n,\overline{\mathbb{Q}}}$, ovvero il gruppo delle radici n-esime dell'unità, su cui $\Gamma_{\mathbb{Q}}$ agisce tramite la sua naturale azione su $\overline{\mathbb{Q}}$.

Dimostrazione: La struttura di gruppo abeliano l'abbiamo studiata con l'Osservazione 3.2.14. L'azione di $\Gamma_{\mathbb{Q}}$ su G è banale, per cui l'azione di $\Gamma_{\mathbb{Q}}$ su $X^*(G)$ è data dall'azione su $\mathbb{G}_m$, che è esattamente quella descritta sopra. □

Gli oggetti presenti nell' Equazione (85) sono in particolare anche $\mathbb{Z}$-moduli. E' dunque possibile applicare all' Equazione (85) il funtore controvariante $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z})$, ottenendo una nuova sequenza esatta, a priori non necessariamente corta. L'idea dietro questo passaggio è che è più facile imporre delle determinate condizioni (come quella sulla base invariante per l'azione di $\Gamma_{\mathbb{Q}}$) al termine centrale di una sequenza esatta corta, per cui questo funtore ci permette di scambiare l'ordine dei moduli con cui stiamo lavorando, come vedremo ora.

Proposizione 3.2.16: Dopo aver applicato il funtore $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z})$ all' Equazione (85) , otteniamo la successione esatta corta di $\mathbb{Z}\big[\Gamma_{\mathbb{Q}}\big]$-moduli

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(M', \mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}}(X^*(G), \mathbb{Z}) \to 0 \tag{86}$$

Dimostrazione: Applicando $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z})$ otteniamo

$$\begin{aligned} 0 \to \mathrm{Hom}_{\mathbb{Z}}(X^*(G), \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(M', \mathbb{Z}) \to \\ \mathrm{Ext}^1_{\mathbb{Z}}(X^*(G), \mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}}(M, \mathbb{Z}) \to \dots \end{aligned} \tag{87}$$

Notiamo che $\mathrm{Hom}_{\mathbb{Z}}(X^*(G), \mathbb{Z}) = 0$ perché $X^*(G)$ è finito. Notiamo inoltre che $\mathrm{Ext}^1_{\mathbb{Z}}(M, \mathbb{Z}) = 0$ perché M è uno $\mathbb{Z}$-modulo libero. Inoltre tutti i termini della nuova sequenza esatta sono $\mathbb{Z}\big[\Gamma_{\mathbb{Q}}\big]$-

moduli in quanto hanno un'azione naturale di $\Gamma_{\mathbb{Q}}$ derivante dall'azione sui termini dell' Equazione (85) . □

Notiamo in particolare che $\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z})$ è isomorfo come $\mathbb{Z}$-modulo a M, mentre l'azione di Galois su $\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z})$ è la duale di quella su M, ovvero $\forall \sigma \in \Gamma_{\mathbb{Q}}, f \in \mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z}),\ \sigma * f(-) = f \circ \sigma^{-1}(-)$. Lo stesso vale per $\mathrm{Hom}_{\mathbb{Z}}(M',\mathbb{Z})$. In particolare

Osservazione 3.2.17: M' ha una $\mathbb{Z}$-base invariante per l'azione di $\Gamma_{\mathbb{Q}}$ se e solo se $\mathrm{Hom}_{\mathbb{Z}}(M',\mathbb{Z})$ ce l'ha.

Dimostrazione: Segue immediatamente dalla caratterizzazione appena fatta dell'azione di Galois su $\mathrm{Hom}_{\mathbb{Z}}(M',\mathbb{Z})$. □

Calcoliamo ora chi è $\mathrm{Ext}^1_{\mathbb{Z}}(X^*(G),\mathbb{Z})$.

Proposizione 3.2.18: $\mathrm{Ext}^1_{\mathbb{Z}}(X^*(G),\mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}(X^*(G),\mathbb{Q}/\mathbb{Z})$ come $\mathbb{Z}\big[\Gamma_{\mathbb{Q}}\big]$-moduli.

Dimostrazione: Consideriamo la sequenza esatta corta di $\mathbb{Z}\big[\Gamma_{\mathbb{Q}}\big]$-moduli (tramite l'azione banale)

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0 \tag{88}$$

Applichiamo ad essa il funtore $\mathrm{Hom}_{\mathbb{Z}}(X^*(G),-)$ ed otteniamo

$$\begin{aligned} 0 \to \mathrm{Hom}_{\mathbb{Z}}(X^*(G),\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(X^*(G),\mathbb{Q}) \to \mathrm{Hom}_{\mathbb{Z}}(X^*(G),\mathbb{Q}/\mathbb{Z}) \to \\ \mathrm{Ext}^1_{\mathbb{Z}}(X^*(G),\mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}}(X^*(G),\mathbb{Q}) \to \dots \end{aligned} \tag{89}$$

Notiamo che $\mathrm{Hom}_{\mathbb{Z}}(X^*(G),\mathbb{Q}) = 0$ perché $X^*(G)$ è un gruppo finito e $\mathrm{Ext}^1_{\mathbb{Z}}(X^*(G),\mathbb{Q}) = 0$ perché $\mathbb{Q}$ è uno $\mathbb{Z}$-modulo iniettivo. Dunque rimane la sequenza

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(X^*(G),\mathbb{Q}/\mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}}(X^*(G),\mathbb{Z}) \to 0 \tag{90}$$

□

In particolare $\mathrm{Ext}^1_{\mathbb{Z}}(X^*(G),\mathbb{Z})$ è finito, da cui segue che

Osservazione 3.2.19: Detto $\tilde{G} := \mathrm{Ext}^1_{\mathbb{Z}}(X^*(G),\mathbb{Z})$, vale $X^*(G) = \mathrm{Ext}^1_{\mathbb{Z}}\big(\tilde{G},\mathbb{Z}\big)$.

Dimostrazione: Applicando il funtore $\mathrm{Hom}_{\mathbb{Z}}(-,\mathbb{Z})$ alla sequenza dell' Equazione (86) , otteniamo

$$\begin{aligned} 0 \to \mathrm{Hom}_{\mathbb{Z}}\big(\tilde{G},\mathbb{Z}\big) \to \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(M',\mathbb{Z}),\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z}),\mathbb{Z}) \to \\ \mathrm{Ext}^1_{\mathbb{Z}}\big(\tilde{G},\mathbb{Z}\big) \to \mathrm{Ext}^1_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(M',\mathbb{Z}),\mathbb{Z}) \to \dots \end{aligned} \tag{91}$$

in cui $\mathrm{Hom}_{\mathbb{Z}}\big(\tilde{G},\mathbb{Z}\big) = 0$ perché $\tilde{G}$ è finito e $\mathrm{Ext}^1_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(M',\mathbb{Z}),\mathbb{Z}) = 0$ perché $\mathrm{Hom}_{\mathbb{Z}}(M',\mathbb{Z})$ è uno $\mathbb{Z}$-modulo libero.
Notiamo inoltre che c'è un'isomorfismo naturale che manda $\mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z}),\mathbb{Z})$ in M e $\mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(M',\mathbb{Z}),\mathbb{Z})$ in M'. Tramite questi isomorfismi naturali, la mappa $\mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(M',\mathbb{Z}),\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z}),\mathbb{Z})$ dell' Equazione (91) viene mandata nella mappa $M' \to M$ dell' Equazione (85) .
Dunque $X^*(G)$ e $\mathrm{Ext}^1_{\mathbb{Z}}\big(\tilde{G},\mathbb{Z}\big)$ sono quozienti di due immersioni naturalmente isomorfe. □

Mettendo insieme i risultati dell'Osservazione 3.2.17 e dell'Osservazione 3.2.19, possiamo concludere che per costruire una sequenza esatta come nell' Equazione (85) ci basta costruire una sequenza esatta corta della forma

$$0 \to N \to N' \to \tilde{G} \to 0 \tag{92}$$

in cui N, N' siano $\mathbb{Z}$-moduli liberi e N' abbia una base invariante per l'azione di $\Gamma_{\mathbb{Q}}$. Infatti da questa possiamo applicare il funtore $\mathrm{Hom}_{\mathbb{Z}}(-,\mathbb{Z})$ ed ottenerne una della forma dell' Equazione (85) .

Per costruire una sequenza come nell' Equazione (92) , procediamo come segue.

Osservazione 3.2.20: L'azione di $\Gamma_{\mathbb{Q}}$ su $\tilde{G}$ si fattorizza tramite l'azione di $\Gamma' := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, dove ζ_n è una radice primitiva n-esima dell'unità.

Dimostrazione: Poiché, per la Proposizione 3.2.18, $\tilde{G} = \mathrm{Hom}_{\mathbb{Z}}(X^*(G), \mathbb{Q}/\mathbb{Z})$ e poiché $\mathbb{Q}/\mathbb{Z}$ è invariante per l'azione di $\Gamma_{\mathbb{Q}}$, notiamo che $\Gamma_{\mathbb{Q}}$ agisce su $\tilde{G}$ solo tramite l'azione su $X^*(G)$, la quale si fattorizza tramite Γ' per l'Osservazione 3.2.15. □

Poniamo allora N' uguale allo $\mathbb{Z}[\Gamma']$-modulo libero generato dagli elementi di $\tilde{G}$, ovvero

$$N' = \bigoplus_{g \in \tilde{G}} \mathbb{Z}[\Gamma'][g] \tag{93}$$

e definiamo la mappa $\varphi : N' \to \tilde{G}$ definita come

$$\sum_{g \in \tilde{G}} a_g[g] \mapsto \sum_{g \in \tilde{G}} a_g * g \tag{94}$$

dove $a_g \in \mathbb{Z}[\Gamma']$ agisce su g tramite la struttura di $\mathbb{Z}[\Gamma']$-modulo di $\tilde{G}$. Sia inoltre $N := \ker(\varphi)$.

Le prossime due osservazioni ci garantiscono che la sequenza esatta corta così costruita rispetti le condizioni richieste, e corrisponda quindi ad una G-isogenia $S \to S'$, completando la dimostrazione del Teorema 3.4.

Osservazione 3.2.21: N' è uno $\mathbb{Z}$-modulo libero e ha una $\mathbb{Z}$-base invariante per l'azione di $\Gamma_{\mathbb{Q}}$.

Dimostrazione: E' chiaro che N' sia uno $\mathbb{Z}$-modulo libero per come l'abbiamo costruito. Per controllare che N' abbia una base invariante per l'azione di $\Gamma_{\mathbb{Q}}$, ci basta verificare che ne abbia una invariante per l'azione di Γ'. Questo è vero perché l'algebra $\mathbb{Z}[\Gamma']$ ha una base invariante per l'azione di Γ', che è quella data dagli elementi di Γ', e di conseguenza anche una somma diretta di alcune copie di $\mathbb{Z}[\Gamma']$ avrà una base invariante. □

Osservazione 3.2.22: N è uno $\mathbb{Z}$-modulo libero.

Dimostrazione: Segue dal fatto che, se A è un dominio a ideali principali, ogni sotto modulo di un A-modulo libero è libero □

§ 3.2.ii.ii. Razionalità del campo delle funzioni razionali di un toro di permutazione —

Per concludere ci manca la dimostrazione del Teorema 3.5. Diamo la seguente caratterizzazione di un toro, dato il suo gruppo dei caratteri su una chiusura algebrica.

Teorema 3.6: Sia L uno $\mathbb{Z}\big[\Gamma_{\mathbb{Q}}\big]$-modulo che sia uno $\mathbb{Z}$-modulo libero in cui l'azione di $\Gamma_{\mathbb{Q}}$ fattorizza tramite l'azione di $G = \mathrm{Gal}(K : \mathbb{Q})$ per una certa estensione di Galois finita K. Il toro $\mathbb{T}$ su $\mathbb{Q}$ tale che $X^*(\mathbb{T}) = L$ è tale che il suo anello delle coordinate sia $K[L]^G$, dove $K[L]$ è la K-algebra generata dagli elementi di L e l'azione φ di G su $K[L]$ è data da

$$\varphi(g)(al) = g(a)(g * l) \tag{95}$$

in cui $g * l$ indica l'azione di G su L. L'azione poi si estende per linearità.
In particolare il campo delle funzioni razionali di $\mathbb{T}$ è $K(L)^G$.

Dimostrazione: [10], Capitolo 3, Sezione 10. □

Ora possiamo procedere con la dimostrazione del Teorema 3.5.

Dimostrazione (Teorema 3.5): Sia S' un toro di permutazione di rango n. Sia $M' = X^*(S')$ il suo gruppo dei caratteri su $\overline{\mathbb{Q}}$. Per ipotesi sappiamo che M' è uno $\mathbb{Z}$-modulo libero con un'azione di $\Gamma_{\mathbb{Q}}$ che agisce per permutazione su una $\mathbb{Z}$-base di M'. Chiamiamo B questa base. Sia $\Omega \subset \Gamma_{\mathbb{Q}}$ il nucleo di quest'azione. In quanto nucleo sarà un sottogruppo normale, quindi esiste un'estensione di Galois $(K : \mathbb{Q})$ per cui vale $\Omega = \mathrm{Gal}\big(\overline{\mathbb{Q}} : K\big)$. Di conseguenza l'azione di $\Gamma_{\mathbb{Q}}$ si fattorizza attraverso l'azione di $G = \mathrm{Gal}(K : \mathbb{Q})$. Supponiamo inizialmente che l'azione di G sia transitiva su $B = \{e_1, ..., e_n\}$. E' facile notare che l'algebra $K(M')$ è isomorfa alla K-algebra dei polinomi di Laurent $K\big[x_1^{\pm 1}, ..., x_n^{\pm 1}\big]$ in cui l'isomorfismo, sui generatori, è dato da

$$\sum_{i=0}^{n} a_i e_i \mapsto x_1^{a_1} x_2^{a_2} ... x_n^{a_n}. \tag{96}$$

Grazie al Teorema 3.6, sappiamo che il campo delle funzioni di S' è $K(x_1, x_2, ..., x_n)^G$. Dunque vogliamo dimostrare che esistono $y_1, ..., y_n \in K(x_1, x_2, ..., x_n)$ algebricamente indipendenti tali che

$$K(x_1, x_2, ..., x_n)^G = \mathbb{Q}(y_1, y_2, ..., y_n). \tag{97}$$

Li costruiamo come segue: sia α un elemento primitivo di $(K : \mathbb{Q})$. Definiamo

$$y_i = \sum_{g \in G} g(\alpha x_i) \tag{98}$$

e notiamo che $g(y_i) = y_i$ per ogni $g \in G$, per cui vale certamente

$$\mathbb{Q}(y_1, y_2, ..., y_n) \subset K(x_1, x_2, ..., x_n)^G. \tag{99}$$

Per ottenere anche l'altra inclusione vogliamo dimostrare che

$$K(x_1, x_2, ..., x_n) = K(y_1, y_2, ..., y_n) \tag{100}$$

perché in questo modo avremmo che

$$K(x_1, x_2, ..., x_n)^G = K(y_1, y_2, ..., y_n)^G = \mathbb{Q}(y_1, y_2, ..., y_n). \tag{101}$$

Per dimostrare l' Equazione (100) chiamiamo N la matrice la cui i-esima riga indica le coordinate di y_i nella base $\{x_1, ..., x_n\}$ (questa frase ha senso solo perché gli y_i stanno nel K-spazio vettoriale generato dagli x_j), ovvero

$$N_{i,j} = \sum_{g \in G_{i,j}} g(\alpha),\ G_{i,j} = \{g \in G |\ g(x_i) = x_j\}. \tag{102}$$

Vogliamo dimostrare che la matrice N è invertibile. Questo implicherebbe che

$$K(x_1, x_2, ..., x_n) = K(y_1, y_2, ..., y_n) \tag{103}$$

perché ci permetterebbe di ottenere gli x_j come combinazioni lineari degli y_i. Per dimostrare che N è invertibile usiamo il Lemma 3.2.23. Verifichiamo le ipotesi del lemma. La j-esima colonna di N è data da

$$\left(\sum_{g \in G_{1,j}} g(\alpha), \sum_{g \in G_{2,j}} g(\alpha), ..., \sum_{g \in G_{n,j}} g(\alpha) \right)^T. \tag{104}$$

Notiamo che, se $h \in G$ è tale che $h(x_j) = x_k$, allora $h(G_{i,j}) = G_{i,k}$, perché

$$h(G_{i,j}) = \{hg \in G |\ g(x_i) = x_j\} = \{g' \in G |\ g'(x_i) = x_k\} = G_{i,k}. \tag{105}$$

Dunque, quando h agisce sulla j-esima colonna di N, che chiamiamo N_j, la manderà in

$$h(N_j) = \left(\sum_{g \in G_{1,k}} g(\alpha), \sum_{g \in G_{2,k}} g(\alpha), ..., \sum_{g \in G_{n,k}} g(\alpha) \right)^T = N_k \tag{106}$$

da cui otteniamo che G permuta le colonne di N. Possiamo anche verificare che una qualsiasi colonna di N ha le entrate linearmente indipendenti su $\mathbb{Q}$ perché, poiché α è un elemento primitivo di $(K : \mathbb{Q})$, abbiamo che i numeri $\{g(\alpha) |\ g \in G\}$ sono tutti linearmente indipendenti tra loro. Di conseguenza anche le entrate di una colonna di N sono linearmente indipendenti su $\mathbb{Q}$, perché una dipendenza lineare tra le entrate di una colonna di N ci darebbe una dipendenza lineare tra i numeri $\{g(\alpha) |\ g \in G\}$.

Nel caso in cui l'azione di G sulla base B di M' non fosse transitiva, supponiamo vi siano r orbite per l'azione di G. Consideriamo nuovamente la K-algebra dei polinomi di Laurent $K\left[x_1^{\pm 1}, ..., x_n^{\pm 1}\right]$ e siano $I_1, I_2, ..., I_r$ gli insiemi degli indici che definiscono le orbite dell'azione di G. Allora, definiamo nuovamente

$$y_i = \sum_{g \in G} g(\alpha x_i) \tag{107}$$

e, per quanto visto nel caso transitivo, abbiamo che

$$K\left(x_{i_1}, x_{i_2}, ..., x_{i_{|I_1|}}\right) = K\left(y_{i_1}, y_{i_2}, ..., y_{i_{|I_1|}}\right) \tag{108}$$

dove $i_1, i_2, ..., i_{|I_1|}$ sono gli elementi di I_1. Lo stesso varrà per tutte le altre orbite. Dunque mettendo insieme questi risultati otteniamo che

$$K(x_1, x_2, ..., x_n) = K(y_1, y_2, ..., y_n) \tag{109}$$

da cui la tesi della prima parte del Teorema 3.5

Per quanto riguarda la regolarità dell'estensione $\mathbb{Q}(S) : \mathbb{Q}(S') = \mathbb{Q}(y_1, ..., y_n)$, supponiamo per assurdo che $\mathbb{Q}(S) \cap \overline{\mathbb{Q}} \neq \mathbb{Q}$. Allora, in maniera analoga alla dimostrazione dell'Osservazione 3.2.3, possiamo dimostrare che la varietà S non è assolutamente irriducibile, il che è assurdo dato che $S_{\overline{\mathbb{Q}}} \equiv \mathbb{G}^n_{m,\overline{\mathbb{Q}}}$ e ha campo delle funzioni razionali $\overline{\mathbb{Q}}(y_1, ..., y_n)$. □

Lemma 3.2.23: Sia $(K : F)$ un'estensione di Galois con gruppo G. Sia $M \in M_{n,n}(K)$ una matrice quadrata a valori in K tale che l'azione di G sulle colonne di M le permuta tra loro. Supponiamo inoltre che le entrate della prima colonna di M siano linearmente indipendenti su F. Allora M è invertibile.

Dimostrazione: [11], Lemma 4. □

sec. 4 — Costruzione esplicita per $\mathbb{Z}/5\mathbb{Z}$

Cerchiamo ora in quest'ultima sezione di utilizzare i mezzi visti nella precedente per costruire in maniera esplicita un rivestimento tra tori con gruppo $A := \mathbb{Z}/5\mathbb{Z}$.

Sia $G := \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ e sia g un generatore di G. Indichiamo con μ_5 il gruppo delle radici quinte dell'unità con la rispettiva azione del Galois. Supponiamo g agisca su μ_5 tramite la mappa $x \to x^3$.
Per comodità di notazione utilizziamo $Y(-)$ per indicare il funtore $\mathrm{Hom}_{\mathbb{Z}}(X^*(-), \mathbb{Z})$, cioè lo $\mathbb{Z}$-duale di $X^*(-)$.

Ricordiamo dalla Osservazione 3.2.20 che l'azione di $\Gamma_{\mathbb{Q}}$ su $Y(A)$ fattorizza tramite G.
Partiamo dallo studiare che $\mathbb{Z}[G]$-modulo è $Y(A)$. Ricordiamo che $Y(A) = \mathrm{Hom}_{\mathbb{Z}}(X^*(A), \mathbb{Q}/\mathbb{Z})$ e che $X^*(A) = \mu_5$. Come gruppo abeliano, $Y(A)$ è isomorfo a $\mathbb{Z}/5\mathbb{Z}$, perché un generatore di $X^*(A)$ dovrà andare in un elemento di $\mathbb{Q}/\mathbb{Z}$ di ordine divisore di 5. Sia a un generatore di $Y(A)$.
Dato $f : \mu_5 \to \mathbb{Q}/\mathbb{Z}$, abbiamo che $(g * f)(x) = f \circ g^{-1}(x) = f(x^2) = 2f(x)$, dunque l'azione di G su $Y(A)$ è l'inversa dell'azione di G su μ_5. In particolare $g * a = 2a$.

Seguendo la costruzione dellla sezione precedente, possiamo scrivere $Y(S') = \bigoplus_{i \in \mathbb{Z}/5\mathbb{Z}} [ia] * \mathbb{Z}[G]$.
Per individuare chi è $Y(S) \subset Y(S')$ utilizziamo la prossima osservazione.

Osservazione 4.0.1: Il sottomodulo $Y(S)$ in $Y(S')$ è lo spazio generato dalle colonne della matrice

$$\begin{pmatrix} 0 & 0 & 0 & -1 & 0 & 0 \\ 2 & 3 & 4 & 5 & 5 & g-2 \\ -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \end{pmatrix} \tag{110}$$

dove la $\mathbb{Z}[G]$-base in cui sono scritte le colonne di questa matrice è quella data da

$$\{[0] * 1, [a] * 1, [2a] * 1, [3a] * 1, [4a] * 1\} =: \{e_0, e_1, e_2, e_3, e_4\} \tag{111}$$

in cui con 1 stiamo indicando $1 \in \mathbb{Z}[G]$.

Dimostrazione: Chiamiamo $v_1, v_2, ..., v_6$ le colonne della matrice. E' facile notare che ogni v_i sta nel nucleo della mappa $\varphi : Y(S') \to Y(A)$, vogliamo dire che ogni elemento del nucleo sta nello spazio generato dai v_i.
Data una qualsiasi combinazione lineare a coefficienti in $\mathbb{Z}[G]$ degli e_i, tramite il quoziente per $\langle v_1, v_2, v_3, v_4 \rangle$ possiamo ridurla ad un elemento di $\mathbb{Z}[G] * e_1$. Dopodiché, se ci scriviamo $\mathbb{Z}[G] = \mathbb{Z} \oplus (g * \mathbb{Z}) \oplus (g^2 * \mathbb{Z}) \oplus (g^3 * \mathbb{Z})$, tramite il quoziente per $\langle v_6 \rangle$ possiamo ridurre il tutto ad un elemento ω di $\mathbb{Z} * e_1$ (qui abbiamo usato che $g * a = 2a$). A questo punto la combinazione lineare iniziale stava in $\ker(\varphi)$ se e solo se ω ci sta, e ω sta nel nucleo se e solo se è nello spazio generato da v_5. □

Dunque, se indichiamo con $L = \langle 5, g-2 \rangle \subset \mathbb{Z}[G]$, otteniamo che

$$Y(S) \cong \mathbb{Z}[G]^4 \oplus L \subset \mathbb{Z}[G]^5 \cong Y(S') \tag{112}$$

in cui l'isomorfismo $Y(S) \cong \mathbb{Z}[G]^4 \oplus L$ è dato da $Y(S) \cong \bigoplus_{i=1}^4 \mathbb{Z}[G] * v_i \ \oplus L$.
Indichiamo con $N = \mathbb{Z}[G] * e_1 \subset Y(S')$ la copia di $\mathbb{Z}[G]$ in cui è immerso L e indichiamo con ψ tale inclusione.
A meno di cambiare la $\mathbb{Z}[G]$-base tramite la quale identifichiamo con $Y(S')$ con $\mathbb{Z}[G]^5$, possiamo fare

in modo che l'inclusione $\mathbb{Z}[G]^4 \oplus L \hookrightarrow \mathbb{Z}[G]^5 = \mathbb{Z}[G]^4 \oplus N$ sia data dall'identità nelle prime 4 coordinate e da ψ nell'ultima componente. Sia $B_{S'}$ la base di $Y(S')$ appena descritta.

4.1. Studiamo L

Prima di proseguire, cerchiamo di capire meglio chi è L.

Osservazione 4.1.1: Se scriviamo $\mathbb{Z}[G]$ come $\mathbb{Z} \oplus (g * \mathbb{Z}) \oplus (g^2 * \mathbb{Z}) \oplus (g^3 * \mathbb{Z})$, possiamo vedere il sottomodulo L come

$$L = \langle g-2, g^2-2g, g^3-2g^2, 5\rangle_{\mathbb{Z}} = \langle g-2, g^2-4, g^3-8, 5\rangle_{\mathbb{Z}} \tag{113}$$

Dimostrazione: Notiamo innanzitutto che

$$\begin{gathered}(g-2)\mathbb{Z}[G] = \langle g-2, g^2-2g, g^3-2g^2, 1-2g^3\rangle_{\mathbb{Z}} = \\ \langle g-2, g^2-2g, g^3-2g^2, 15\rangle_{\mathbb{Z}}\end{gathered} \tag{114}$$

Ci chiediamo chi sia $L/(g-2)\mathbb{Z}[G] = ((g-2)\mathbb{Z}[G] + 5\mathbb{Z}[G])/(g-2)\mathbb{Z}[G]$.
Sia l un elemento di $5\mathbb{Z}[G]$, ovvero $l = 5(a_1 + a_2 g + a_3 g^2 + a_4 g^3)$ con $a_i \in \mathbb{Z}$. Allora anche

$$\begin{gathered}l' = l - 5a_4(g^3-2g^2) - 5(a_3+2a_4)(g^2-2g) - 5(a_2+2a_3+4a_4)(g-2) = \\ 5(a_1+2a_2+4a_3+8a_4)\end{gathered} \tag{115}$$

starà in $5\mathbb{Z}[G]$. Facendo la divisione con resto di l' per 15, possiamo rimanere con un resto di 0, 5 o 10. Dunque se a $(g-2)\mathbb{Z}[G]$ aggiungessimo $5\mathbb{Z}$ otterremmo tutto L, da cui la tesi. □

Osservazione 4.1.2: Chiamiamo B_L la $\mathbb{Z}$-base di L data da $\{5, g-2, g^2-4, g^3-8\}$ e chiamiamo B_N la $\mathbb{Z}$-base di N data da $\{1, g-2, g^2-4, g^3-8\}$. Notiamo che nelle basi B_L e B_N la mappa ψ è esprimibile tramite la matrice

$$\begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{116}$$

Osservazione 4.1.3: In particolare nella base B_L l'azione di g su L è data dalla matrice

$$\begin{pmatrix} 2 & 0 & 0 & -3 \\ 5 & -2 & -4 & -8 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{117}$$

4.2. Ridursi a N' e L'

Vogliamo ora capire chi sono $X^*(S')$, $X^*(S)$ e l'inclusione $X^*(S') \hookrightarrow X^*(S)$. Ricordiamo che $X^*(S')$ e $X^*(S)$ sono gli $\mathbb{Z}$-duali di $Y(S')$ e $Y(S)$.
Indichiamo con M' lo $\mathbb{Z}$-duale di uno $\mathbb{Z}[G]$-modulo M. E' facile notare che $\mathbb{Z}[G]' \cong \mathbb{Z}[G]$.
Dunque la duale della mappa $Y(S) \hookrightarrow Y(S')$, data da

$$\mathbb{Z}[G]^4 \oplus L \xhookrightarrow{(\mathrm{id} \oplus \psi)} \mathbb{Z}[G]^4 \oplus N$$

sarà $X^*(S') \hookrightarrow X^*(S)$ e sarà data da

$$\mathbb{Z}[G]^4 \oplus N' \xhookrightarrow{(\mathrm{id} \oplus \psi')} \mathbb{Z}[G]^4 \oplus L'$$

In particolare, la sequenza esatta corta

$$0 \to X^*(S') \to X^*(S) \to X^*(A) \to 0 \tag{118}$$

diventa

$$0 \to \mathbb{Z}[G]^4 \oplus N' \to \mathbb{Z}[G]^4 \oplus L' \to X^*(A) \to 0 \tag{119}$$

la quale, poiché la seconda freccia di questa sequenza è $\mathrm{id} \oplus \psi'$, è equivalente a

$$0 \to N' \to L' \to X^*(A) \to 0 \tag{120}$$

Osservazione 4.2.1: N' e L' sono $\mathbb{Z}$-moduli liberi. In più, N' ha una $\mathbb{Z}$-base invariante per l'azione di $\Gamma_{\mathbb{Q}}$. Dunque la sequenza esatta (27) è della forma di quella nell' Equazione (85) , e quindi corrisponde ad un rivestimento regolare da un toro ad un toro di permutazione con gruppo A.

Dimostrazione: E' immediato verificare che N' e L' sono $\mathbb{Z}$-moduli liberi. Inoltre la $\mathbb{Z}$-base $B = \{1, g, g^2, g^3\}$ è una $\mathbb{Z}$-base per N invariante per l'azione di $\Gamma_{\mathbb{Q}}$ e quindi la sua $\mathbb{Z}$-base duale $B' = \{x_1, x_2, x_3, x_4\}$ sarà una $\mathbb{Z}$-base invariante di N'. □

4.3. Studiamo N' e L'

D'ora in poi, quando parleremo di basi dei moduli N' e L' ci riferiremo sempre a $\mathbb{Z}$-basi, anche se non lo specifichiamo di volta in volta.

Osservazione 4.3.1: Sia $B_{L'} = \{\delta_1, \delta_2, \delta_3, \delta_4\}$ la base di L' duale di B_L. Analogamente, sia $B_{N'} = \{w_1, w_2, w_3, w_4\}$ la base di N' duale di B_N. Allora notiamo che la mappa ψ', nelle basi $B_{N'}$ e $B_{L'}$, è esprimibile tramite la matrice

$$\begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{121}$$

Dimostrazione: La matrice che esprime la mappa ψ' nelle basi $B_{N'}$ e $B_{L'}$ è la trasposta della matrice che esprime la mappa ψ, nelle basi B_N e B_L. Dunque concludiamo per l'Osservazione 4.1.2. □

Osservazione 4.3.2: Nella base $B_{L'}$ l'azione di g^{-1} su L' è data dalla matrice

$$\begin{pmatrix} 2 & 5 & 0 & 0 \\ 0 & -2 & 1 & 0 \\ 0 & -4 & 0 & 1 \\ -3 & -8 & 0 & 0 \end{pmatrix} \tag{122}$$

Dimostrazione: Segue dall'Osservazione 4.1.3 unita al fatto che la matrice che rappresenta l'azione g^{-1} nella rappresentazione duale è la trasposta della matrice che rappresenta l'azione di g su L. □

Osservazione 4.3.3: Dall'Osservazione 4.3.1 otteniamo che $L' = N' + \langle \delta_1 \rangle_{\mathbb{Z}}$ (stiamo identificando N' con la sua immagine tramite ψ', d'ora in poi quando parleremo di N' lo penseremo sempre immerso in L'). Inoltre $\delta_1 \notin N'$, ma $5\delta_1 \in N'$.

Osservazione 4.3.4: In N' al momento abbiamo definito due basi: $B_{N'}$, che è comoda perché ci permette di scrivere bene l'immersione di N' in L', e B' che è utile perché è una base invariante per l'azione di G. Analizziamo qual è la matrice di cambio base tra queste due.
La matrice di cambio base da $B_{N'}$ a B' è

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 4 & 0 & 1 & 0 \\ 8 & 0 & 0 & 1 \end{pmatrix} \tag{123}$$

In particolare abbiamo che

$$\begin{aligned} 5\delta_1 = w_1 &= x_1 + 2x_2 + 4x_3 + 8x_4 \\ \delta_2 = w_2 &= x_2 \\ \delta_3 = w_3 &= x_3 \\ \delta_4 = w_4 &= x_4 \end{aligned} \tag{124}$$

Dimostrazione: E' facile calcolare che matrice di cambio base da B a B_N è

$$\begin{pmatrix} 1 & 2 & 4 & 8 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{125}$$

e la matrice sui duali di cambio base tra le basi duali è la trasposta. □

4.4. Calcoliamo $\mathbb{Q}(T_N)$ e $\mathbb{Q}(T_L)$

Siano T_N e T_L i tori i cui gruppi dei caratteri su $\overline{\mathbb{Q}}$ sono rispettivamente N' e L'.

Osservazione 4.4.1: $\mathbb{Q}(T_L) : \mathbb{Q}(T_N)$ è un'estensione di Galois con gruppo A. Inoltre il campo $\mathbb{Q}(T_N)$ è un campo della forma $\mathbb{Q}(t_1, t_2, t_3, t_4)$, con t_1, t_2, t_3, t_4 algebricamente indipendenti.

Dimostrazione: Poiché li abbiamo ottenuti da una sequenza della forma di quella dell' Equazione (85) , abbiamo che T_N è il quoziente di T_L per un'azione di A, dunque la mappa $T_L \to T_N$ data dal quoziente è un rivestimento di Galois con gruppo A.
La seconda parte deriva dal fatto che T_N è un toro di permutazione (Osservazione 4.2.1) unito al Teorema 3.5. □

L'obiettivo di questa sezione sarà studiare l'estensione di Galois $\mathbb{Q}(T_L) : \mathbb{Q}(T_N)$ e in particolare trovare (in una forma più o meno esplicita, come vedremo più avanti) un polinomio a coefficienti in $\mathbb{Q}(T_N) = \mathbb{Q}(t_1, t_2, t_3, t_4)$ di cui questo è campo di spezzamento. Se trovassimo un tale polinomio poi potremmo specializzare le variabili t_1, t_2, t_3, t_4 ad infinite 4-uple di numeri razionali in modo da ottenere dei polinomi in $\mathbb{Q}[x]$ con gruppo di Galois A, come visto nella Sezione 2.2.

Sia $K = \mathbb{Q}(\zeta_5)$. I caratteri, in quanto tali, sono funzioni razionali e in particolare i caratteri in N' e in L', poiché l'azione di $\Gamma_{\mathbb{Q}}$ su N' e su L' fattorizza tramite G, sono funzioni razionali definite su K.

Osservazione 4.4.2: Ricordiamo che nella Definizione 3.1.8 avevamo definito la struttura di gruppo abeliano per il gruppo dei caratteri tramite la moltiplicazione, ovvero dati due caratteri χ, χ' abbiamo definito $(\chi + \chi')(h) = \chi(h) * \chi'(h)$. Nei moduli N' e L' abbiamo tenuto la notazione addittiva, però d'ora in poi dovremo utilizzare la notazione moltiplicativa, perché lavoreremo con i campi delle funzioni razionali, sui quali l'operazione che rende N' e L' degli $\mathbb{Z}$-moduli è la moltiplicazione.

Per il Teorema 3.6 sappiamo che $\mathbb{Q}(T_N) = K(N')^G$ e $\mathbb{Q}(T_L) = K(L')^G$. In particolare, poiché B' genera N', abbiamo che

$$K(N') = K(x_1, x_2, x_3, x_4) \tag{126}$$

e analogamente, sfruttando le relazioni date dall' Equazione (124) , abbiamo

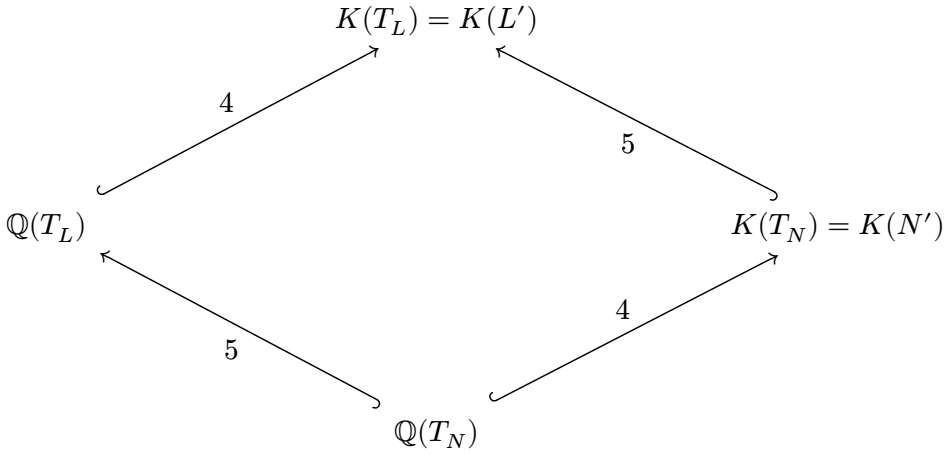
$$K(L') = K(\delta_1, \delta_2, \delta_3, \delta_4) = K(\delta_1, x_2, x_3, x_4) = K(N')(\delta_1) \tag{127}$$

in cui l'elemento δ_1 è radice del polinomio minimo $\delta_1^5 = x_1 x_2^2 x_3^4 x_4^8$.

Osservazione 4.4.3: $K(L') : K(N')$ è un'estensione di Galois. Inoltre $1, \delta_1, \delta_1^2, \delta_1^3, \delta_1^4$ è una $K(N')$ -base di $K(L')$.

Dimostrazione: La prima affermazione deriva dal fatto che le altre radici del polinomio minimo di δ_1 sono gli elementi $\zeta_5^i \delta_1$ con $0 \leq i \leq 4$, i quali stanno in $K(N')(\delta_1)$. La seconda deriva dal fatto che δ_1 genera l'estensione $K(L') : K(N')$ e il suo polinomio minimo ha grado 5. □

Dunque abbiamo le seguenti composizioni estensioni di Galois di campi, in cui sulle frecce sono indicati i gradi delle estensioni,



In particolare, notiamo che $K(T_N) \cap \mathbb{Q}(T_L) = \mathbb{Q}(T_N)$, perché il grado dell'estensone data dall'intersezione deve dividere sia 4 sia 5, per cui l'intersezione deve essere banale. Inolte, $K(T_L) : \mathbb{Q}(T_N)$ è di Galois perché è la composizione di due estensioni di Galois.

Osservazione 4.4.4: Per l'Osservazione 4.2.1 sappiamo che T_N è un toro di permutazione, dunque la dimostrazione di Teorema 3.5 ci dà un procedimento costruttivo per ottenere dei generatori di $\mathbb{Q}(T_N)$. Abbiamo che $\mathbb{Q}(T_N) = \mathbb{Q}(y_1, y_2, y_3, y_4)$, dove y_1, y_2, y_3, y_4 sono definiti come

$$y_i = \sum_{g \in G} g(\alpha x_i) \tag{128}$$

con α generatore dell'estensione $K : \mathbb{Q}$. Se scegliamo $\alpha = \zeta_5$ otteniamo i seguenti y_i:

$$\begin{aligned} y_1 &= \zeta_5 x_1 + \zeta_5^3 x_2 + \zeta_5^4 x_3 + \zeta_5^2 x_4 \\ y_2 &= \zeta_5^2 x_1 + \zeta_5 x_2 + \zeta_5^3 x_3 + \zeta_5^4 x_4 \\ y_3 &= \zeta_5^4 x_1 + \zeta_5^2 x_2 + \zeta_5 x_3 + \zeta_5^3 x_4 \\ y_4 &= \zeta_5^3 x_1 + \zeta_5^4 x_2 + \zeta_5^2 x_3 + \zeta_5 x_4 \end{aligned} \tag{129}$$

Notiamo che da questa scrittura siamo anche in grado di ricavare x_1, x_2, x_3, x_4 come combinazioni lineari di y_1, y_2, y_3, y_4.

Ora vogliamo trovare un generatore dell'estensione $\mathbb{Q}(T_L) : \mathbb{Q}(T_N)$, in modo da poi calcolarne il polinomio minimo, il quale avrà necessariamente $\mathbb{Q}(T_L)$ come campo di spezzamento. In particolare, qualsiasi elemento di $\mathbb{Q}(T_L) \setminus \mathbb{Q}(T_N)$ genererà l'estensione, perché l'estensione generata da un elemento di questo tipo deve avere grado maggiore di 1 e divisore di 5, per cui è necessariamente 5.

Osservazione 4.4.5: L'elemento $d = \sum_{g \in G} g(\delta_1)$ sta in $\mathbb{Q}(T_L) \setminus \mathbb{Q}(T_N)$ e quindi genera l'estensione $\mathbb{Q}(T_L) : \mathbb{Q}(T_N)$.

Dimostrazione: E' evidente che d stia in $\mathbb{Q}(T_L)$ perché è invariante per l'azione di G. Inoltre, grazie all'Osservazione 4.3.2, possiamo calcolare chi sono $g^{-1}(\delta_1), g^2(\delta_1), g(\delta_1)$. Usando le relazioni date da Equazione (124) , otteniamo

$$\begin{aligned} g^{-1}(\delta_1) &= \delta_4^{-3}\delta_1^2 = x_4^{-3}\delta_1^2 \\ g^2(\delta_1) &= \delta_3^{-3}\delta_4^{-6}\delta_1^4 = x_3^{-3}x_4^{-6}\delta_1^4 \\ g(\delta_1) &= \delta_2^{-3}\delta_3^{-6}\delta_4^{-12}\delta_1^8 = x_1 x_2^{-1} x_3^{-2} x_4^{-4}\delta_1^3 \\ d &= \delta_1 + x_4^{-3}\delta_1^2 + x_3^{-3}x_4^{-6}\delta_1^4 + x_1 x_2^{-1} x_3^{-2} x_4^{-4}\delta_1^3. \end{aligned} \tag{130}$$

In particolare, poiché $1, \delta_1, \delta_1^2, \delta_1^3, \delta_1^4$ formano una $K(N')$-base di $K(L')$, notiamo che $\delta_1, g^{-1}(\delta_1), g^2(\delta_1), g(\delta_1)$ sono tutti linearmente indipendenti su $K(N')$ e nessuno di loro sta in $K(N')$, quindi la loro somma, cioè d, non sta in $K(N')$ e di conseguenza neanche in $\mathbb{Q}(T_N)$. □

Dunque abbiamo un generatore dell'estensione $\mathbb{Q}(T_L) : \mathbb{Q}(T_N)$. Ora ci manca calcolarne il polinomio minimo. Per farlo sfruttiamo le prossime due osservazioni.

Osservazione 4.4.6: Detto $H = \mathrm{Gal}(K(T_L) : K(T_N))$, abbiamo che il polinomio minimo di d su $\mathbb{Q}(T_N)$ è dato da

$$p(z) = \prod_{h \in H} (z - h(d)) \tag{131}$$

Dimostrazione: Ci basta verificare che i coefficienti di $p(z)$ stiano sia in $\mathbb{Q}(T_L)$, sia in $K(T_N)$, così staranno nell'intersezione che è $\mathbb{Q}(T_N)$ (dopodiché $p(z)$ sarà necessariamente il polinomio minimo di d perché ha grado 5). Poiché $p(z)$ è invariante per l'azione di H, i coefficienti stanno in $K(T_N)$.

D'altra parte H è un sottogruppo di $\mathrm{Gal}(K(T_L) : \mathbb{Q}(T_N))$ e in particolare l'azione di H manderà d nelle sue radici coniugate su $\mathbb{Q}(T_N)$, le quali stanno in $\mathbb{Q}(T_L)$ (perché $\mathbb{Q}(T_L) : \mathbb{Q}(T_N)$ è di Galois). Dunque $h(d) \in \mathbb{Q}(T_L)$ e quindi $p(z)$ è anche a coefficienti in $\mathbb{Q}(T_L)$. □

Osservazione 4.4.7: Utilizzando quanto detto finora, siamo in grado di calcolare i coefficienti di $p(z)$ esplicitamente in funzione di x_1, x_2, x_3, x_4. Inoltre, poiché sappiamo esprimere x_1, x_2, x_3, x_4 in funzione di y_1, y_2, y_3, y_4 e poiché i coefficienti di $p(z)$ stanno in $\mathbb{Q}(T_N) = \mathbb{Q}(y_1, y_2, y_3, y_4)$, siamo in grado di scrivere esplicitamente $p(z)$ come polinomio a coefficienti in $\mathbb{Q}(y_1, y_2, y_3, y_4)$.

Nota: utilizziamo il termine "essere in grado" di proposito, per far capire al lettore cosa potremmo ottenere con una potenza di calcolo sufficientemente alta, usando solo ciò che abbiamo ricavato in questa sezione. Abbiamo calcolato i coefficienti di $p(z)$ in funzione di y_1, y_2, y_3, y_4 con MAGMA[2], un programma ideato per eseguire conti algebrici, e il risultato veniva di svariate pagine. Dunque per ora ci concentriamo su cosa siamo in grado di calcolare, senza riportare gli effettivi risultati in questa tesi. Successivamente calcoleremo un polinomio in due variabili, che possiamo vedere come polinomio di quinto grado a coefficienti in $\mathbb{Q}(t)$ con gruppo di Galois A su $\mathbb{Q}(t)$.

Dimostrazione: Notiamo innanzitutto che sappiamo esprimere gli elementi della forma $h(d)$ con $h \in H$ esplicitamente in funzione di $\delta_1, x_1, x_2, x_3, x_4$. Questo perché l'estensione $K(T_L) : K(T_N)$ è generata da δ_1 e le altre radici del suo polinomio minimo sono $\zeta_5^i \delta_1$. Poiché H ha ordine 5 e il polinomio minimo di δ_1 è di quinto grado, il gruppo deve essere ciclico ed è generato da un elemento $\tilde{h}$ tale che $\tilde{h}(\delta_1) = \zeta_5 \delta_1$. Per cui vale $\tilde{h}^i(\delta_1) = \zeta_5^i \delta_1$ e

$$\tilde{h}^i(d) = \zeta_5^i \delta_1 + x_4^{-3} \zeta_5^{2i} \delta_1^2 + x_3^{-3} x_4^{-6} \zeta_5^{4i} \delta_1^4 + x_1 x_2^{-1} x_3^{-2} x_4^{-4} \zeta_5^{3i} \delta_1^3. \tag{132}$$

Dunque siamo in grado di calcolare esplicitamente

$$p(z) = \prod_{0 \le i \le 4} \left(z - \tilde{h}^i(d) \right). \tag{133}$$

Sfruttando la Equazione (132) , notiamo che i coefficienti di $p(z)$ sono tutti polinomi in $K(x_1, x_2, x_3, x_4)[\delta_1]$. Sia p_j il coefficiente di grado j di $p(z)$. Notiamo che, sfruttando il fatto che vale $\delta_1^5 = x_1 x_2^2 x_3^4 x_4^8$, possiamo scrivere

$$p_j = \sum_{0 \le i \le 4} c_i(x_1, x_2, x_3, x_4) \delta_1^i \text{ con } c_i(x_1, x_2, x_3, x_4) \in K(T_N). \tag{134}$$

Poiché $p_j \in K(T_N)$ notiamo che i coefficienti dei termini con $i \neq 0$ devono essere nulli. Dunque $p_j = c_0(x_1, x_2, x_3, x_4)$. Inoltre, poiché per l'Osservazione 4.4.4 sappiamo scrivere x_1, x_2, x_3, x_4 come combinazioni lineari di y_1, y_2, y_3, y_4, allora siamo anche in grado di scrivere $p_j = c'(y_1, y_2, y_3, y_4)$ con $c'(y_1, y_2, y_3, y_4) \in K(y_1, y_2, y_3, y_4)$.
D'altra parte sappiamo che $p_j \in \mathbb{Q}(T_N) = \mathbb{Q}(y_1, y_2, y_3, y_4)$, quindi c' deve in realtà essere una funzione razionale a coefficienti in $\mathbb{Q}$. Dunque, se avessimo svolto i conti che abbiamo descritto, avremmo scritto esplicitamente $p(z)$ come polinomio a coefficienti in $\mathbb{Q}(y_1, y_2, y_3, y_4)$. □

Notiamo anche che, a meno di moltiplicare tutto per un denominatore comune, possiamo assumere che $p(z)$ sia a coefficienti in $\mathbb{Q}[y_1, y_2, y_3, y_4]$, ovvero che possiamo vedere p come un polinomio nelle variabili y_1, y_2, y_3, y_4, z a coefficienti in $\mathbb{Q}$. Con abuso di notazione chiamiamo $p(y_1, y_2, y_3, y_4, z)$ questo polinomio.

[2] http://magma.maths.usyd.edu.au/magma/

4.5. Troviamo un polinomio in due variabili con gruppo di Galois $\mathbb{Z}/5\mathbb{Z}$

Ciò che faremo in quest'ultima sottosezione è cercare un polinomio irriducibile $q(x,y) \in \mathbb{Q}[x,y]$ tale che il gruppo di Galois del suo campo di spezzamento su $\mathbb{Q}(y)$ sia $A = \mathbb{Z}/5\mathbb{Z}$ e tale che il suo campo di spezzamento sia un'estensione regolare di $\mathbb{Q}(y)$.

Osservazione 4.5.1: Se queste due ipotesi sono verificate possiamo concludere, grazie al Teorema 2.7, che è possibile specializzare y a infiniti numeri razionali y_0 in modo tale che il polinomio $q(x,y_0) \in \mathbb{Q}[x]$ abbia ancora A come gruppo di Galois. Inoltre, grazie alla Proposizione 3.2.2, sappiamo che al variare di y_0 troviamo infiniti campi di spezzamento distinti per i polinomi $q(x,y_0)$.

Osservazione 4.5.2: $\mathbb{Q}(T_L) : \mathbb{Q}(T_N)$ è un'estensione regolare.

Dimostrazione: Segue dalla seconda affermazione del Teorema 3.5. □

Osservazione 4.5.3: Grazie al Corollario 3.3.1, notiamo che dall'estensione regolare $\mathbb{Q}(T_L) : \mathbb{Q}(T_N)$ possiamo ottenere un rivestimento di Galois regolare di $\mathbb{P}^1$ con gruppo A.
Per farlo dobbiamo trovare un rivestimento regolare $X \to W$, con X birazionalmente equivalente a T_L e W aperto denso di $\mathbb{P}^4$, indotto dall'estensione $\mathbb{Q}(T_L) : \mathbb{Q}(T_N) = \mathbb{Q}(y_1, ..., y_4)$. Per il Teorema 3.3 sappiamo che scegliendo una retta generica in $\mathbb{P}^4$ e restringendoci a guardare il rivestimento su questa retta esso sarà regolare e di Galois con gruppo A.

In particolare possiamo definire

$$W = \mathbb{A}^4 \quad \text{e } X = \{(y_1, y_2, y_3, y_4, z) \in W \times \mathbb{A}^1 | p(y_1, y_2, y_3, y_4, z) = 0\} \subset W \times \mathbb{A}^1, \quad (135)$$

che ci forniscono il rivestimento di Galois regolare $f : X \to W$ dato dalla restrizione a X della proiezione di $W \times \mathbb{A}^1 \to W$.

Proposizione 4.5.4: Data la retta l, parametrizzata da

$$y_1 = y, y_2 = 1, y_3 = 0, y_4 = 0, \quad (136)$$

questa ci dà un rivestimento $f^{-1}(l) \to l$, in cui

$$f^{-1}(l) = \{(y,z) \in \mathbb{A}^1 \times \mathbb{A}^1 | p(y,1,0,0,z) = 0\}. \quad (137)$$

In particolare, il polinomio $p(y,1,0,0,z) \in \mathbb{Q}(y)[z]$ è irriducibile e il suo campo di spezzamento su $\mathbb{Q}(y)$ è un'estensione regolare con gruppo di Galois A.
Inoltre, utilizzando i ragionamenti fatti nell'Osservazione 4.4.7, possiamo calcolare esplicitamente, grazie all'aiuto del software MAGMA, $p(y,1,0,0,z)$, che viene

$$p(y,1,0,0,z) = z^5 + \frac{1}{125}(-1y^6 - 3y^5 - 7y^4 - 9y^3 - 8y^2 - 4y - 1)z^3 + \frac{1}{3125}(4y^7 + 12y^6 + 25y^5 + 30y^4 + 20y^3 + 7y^2 + 1y)z^2 + \frac{1}{390625}(4y^{12} + 9y^{11} - 14y^{10} - 75y^9 - 135y^8 - 46y^7 + 254y^6 + 526y^5 + 525y^4 + 320y^3 + 126y^2 + 31y + 4)z + \frac{1}{48828125}(-7y^{15} - 12y^{14} + 36y^{13} + 137y^{12} + 169y^{11} - 120y^{10} - 732y^9 - 1104y^8 - 918y^7 - 691y^6 - 816y^5 - 913y^4 - 661y^3 - 287y^2 - 69y - 7) \quad (138)$$

Dimostrazione: Per controllare che il polinomio sia irriducibile e abbia gruppo di Galois uguale ad A ci basta controllare che questo sia vero per una specializzazione di y ad un qualche numero razionale y_0. Questo perché se $p(y,1,0,0,z)$ fosse riducibile, allora anche la sua specializzazione lo sarebbe. Inoltre, valgono le ipotesi del Teorema 2.8, perché

$$\mathrm{Gal}(p(y_0,1,0,0,z)) = A = \mathrm{Gal}(p(y_1,y_2,y_3,y_4,z)), \quad (139)$$

dunque il Teorema 2.8 ci dice che anche $\mathrm{Gal}(p(y,1,0,0,z)) = A$.
MAGMA ci permette di verificare che esista una specializzazione di y per cui il polinomio $p(y_0,1,0,0,z)$ è irriducibile e con gruppo di Galois A, e in effetti esiste.

Ci rimane da verificare che il campo di spezzamento F di $p(y,1,0,0,z)$ su $\mathbb{Q}(y)$ sia un'estensione regolare. Supponiamo che non lo sia, ovvero se $F \cap \overline{\mathbb{Q}} = F' \neq \mathbb{Q}$, allora avremmo $\mathbb{Q}(y) \subset F'(y) \subseteq F$. Poiché $F : \mathbb{Q}(y)$ ha grado 5, notiamo che dobbiamo per forza avere $F'(y) = F$. Dunque in $F'(y)$ possiamo scrivere

$$p(y,1,0,0,z) = \prod_{1 \leq i \leq 5} (z - r_i(y)) \quad (140)$$

con $r_i(y) \in F'(y)$. Ne segue che, quando specializziamo y a $y_0 \in \mathbb{Q}$, possiamo scrivere

$$p(y_0,1,0,0,z) = \prod_{1 \leq i \leq 5} (z - r_i(y_0)) \quad (141)$$

con $r_i(y_0) \in F'$. Dunque in particolare $p(y_0,1,0,0,z)$ si spezza in F' e quindi F' contiene il campo di spezzamento di $p(y_0,1,0,0,z)$ su $\mathbb{Q}$. Quindi per verificare che $F : \mathbb{Q}(y)$ sia regolare ci basta trovare due specializzazioni y_0 e $y_{0'}$ per cui i campi di spezzamento di $p(y_0,1,0,0,z)$ e $p(y_{0'},1,0,0,z)$ su $\mathbb{Q}$ siano distinti e di grado 5, perché, avendo $F' : \mathbb{Q}$ grado 5, non li potrebbe contenere entrambi. Sempre tramite MAGMA, abbiamo verificato che questo accada, dunque $F : \mathbb{Q}(y)$ è regolare. □

Dunque abbiamo costruito un polinomio $\tilde{p}(y,z) = p(y,1,0,0,z) \in \mathbb{Q}[y,z]$ tale che al variare delle specializzazioni di y a $y_0 \in \mathbb{Q}$ otteniamo infiniti polinomi con campi di spezzamento distinti, tutti con gruppo di Galois su $\mathbb{Q}$ uguale a $\mathbb{Z}/5\mathbb{Z}$.

sec. 5 — Bibliografia

[1] J.-P. Serre, *Topics in Galois Theory*, 2nd ed. Boca Raton: A K Peters/CRC Press, 2007.

[2] K. J. Nowak, «Some elementary proofs of Puiseux's theorems», *Universitatis Iagellonicae Acta Mathematica*, vol. 48, pp. 279–282, 2000.

[3] J. S. Milne, «Algebraic Groups (v2.00)». 2015.

[4] R. Hartshorne, *Algebraic Geometry*. New York: Springer, 1977.

[5] T. Stacks project authors, «The Stacks project». [Online]. Disponibile su: https://stacks.math.columbia.edu/tag/030U

[6] I. R. Shafarevich, *Basic Algebraic Geometry 1: Varieties in Projective Space*. Springer Berlin, Heidelberg, 2013.

[7] Y. Zhao, «Géométrie Algébrique et Géométrie Analytique», nov. 2013.

[8] T. Stacks project authors, «The Stacks project». [Online]. Disponibile su: https://stacks.math.columbia.edu/tag/02KH

[9] R. Vakil, «The Rising Sea, Foundations of Algebraic Geometry». 2017.

[10] M. Lorenz, *Multiplicative Invariant Theory*, vol. 135. in Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics, vol. 135. Springer, 2005.

[11] A. Jamshidpey, N. Lemire, e E. Schost, «Algebraic Construction of Quasi-split Algebraic Tori». gennaio 2018.